Distributed systems security governance, a SOA based approach

Pierre de Leusse */**, David Brossard **

* Newcastle University; ** BT Innovate

Pierre.de-leusse@ncl.ac.uk

1 Introduction

The aim of this demonstration is to show how governed composition of security related services, provided through the Security as a Service (SaaS) paradigm, can be leveraged on in order to provide a more flexible and usable approach to security in distributed and complex systems.

The demonstration will feature the presentation of a security governance gateway that allows manipulating the security configuration of resources exposed through it in a more dynamic way compared to existing techniques. An additional key aspect of the governance gateway is to improve the visibility of the different parameters to take in account when securing the access to a resource in order to make the decision process more adequate. Through this presentation, the demonstrators hope to show the practicability and interest of governed, composable and adaptable security.

1.1 Objectives of SOA security governance

Functional decomposition into services, reuse, loose coupling, and distribution of resources are all perceived benefits of the investment on SOA. This malleability can also bring about the risk of a more difficult oversight. The same service is used in different applications the infrastructure will have to adapt to these different contexts of use in order to provide variations in required functionality, varying quality of service, varying billing schemes, and meet varying security requirements. Achieving such variations in a cost efficient way can be achieved by composing the core business function offered by a service with other services implementing infrastructure capabilities that fulfil varying non-functional requirements.

However, as the number of services increases and their use in different contexts proliferates, it becomes necessary to automate policy enforcement and compliance monitoring. Furthermore, the composition of services into different business applications over a common infrastructure intensifies the need for end-to-end monitoring and analysis to assess the business performance impact. Managing the full life-cycle of service definition, deployment, exposure and operation requires management processes that take into account their composition with the infrastructure capabilities that take of non-functional requirements. Finally, policies may change during the life-time of a service. Policy updates may be the result of various reasons including business optimisation, of reaction to new business opportunities, of risk / threat mitigation, of operational emergencies, etc. It becomes therefore clear that a well designed governance framework is a prerequisite to successfully implementing a SOA. The authors are involved in an activity at BT Innovate that is developing such a governance framework focusing on fulfilling security and dependability requirements in Service Oriented Infrastructures. More details on the objectives of such a SOA governance framework are given in [1].

1.2 Anatomy of governance framework

The presentation will be a live demonstration of composable and flexible security using connected systems.

The presenters have developed a SOA based infrastructure for security governance that meets the requirements and specifications introduced in [2][3][4].

In order to demonstrate the security governance, the authors have developed a security gateway that manages the security of web services that are exposed through it by the way of a security profile.

The security profile is defined by a taxonomy, presented in Figure 1, that describes the set of infrastructure services that are required for security (e.g. policy enforcement point, identity management, access control). This taxonomy is completed by sets of additional constraints such as policy templates; inter infrastructures coordination and management processes. Managed, these elements allow dynamically selecting and composing appropriate services to provide security and change it on the fly when necessary (e.g. detection of a security threat, change of requirements).

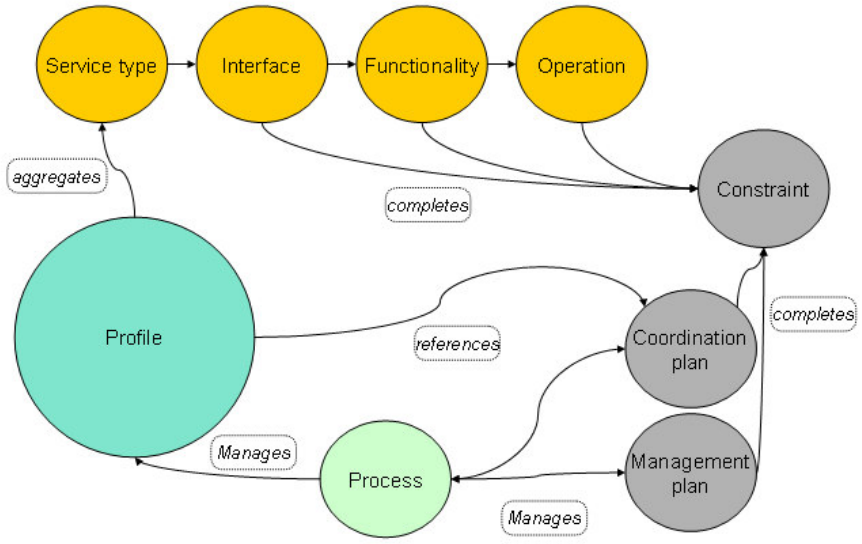

Figure 1. Profile description taxonomy

1.3 Benefits and Unique Selling Points of the solution

The innovations of the SOA based security governance demonstration is the increased usability it brings to security for non specialists that just want to expose their resources in a secured way, the semantically enhanced management capability to configure security at an abstract or more concrete level for security professionals, the improved visibility of consumed resources' security related properties it and finally the added flexibility to security management it allows. In addition, many different distributed systems such as services or mashups can make use of the security governance infrastructure presented.

One of the main innovations of the selected architecture is its modularity. Indeed, being based on a SOA makes possible to manage each module independently as is possible for Web services. In addition, this allows applying the same advantages provided to the supported SOA to the SOI-GGW itself. This concretely translates into

a higher reliability and security in addition to the flexibility gain. Finally, using a SOA allows rendering the SOI-GGW extendable in case supplementary requirements should arise.

Another innovation is that this solution aims at addressing the issue of business capability exposure and management, unlike most other frameworks that only target the visibility, policy management and administration or resource life-cycle management.

An additional innovation stems from the fact that negotiation with different governance frameworks is thought of from the start. Where other governance solutions offer interoperability based upon the use of programmable API, shared interface exposed on the network or even for WSRR, the SOI-GGW proposed a policy and well defined schemes driven approach on the top of its SOA. These two elements put together offer a high interoperability from the semantic and technical points of view in both operational and managerial sides of the governance.

The final innovation brought by the security governance model adopted is that it allows managing many different types of services in various contexts. This is made possible by the SOA used to model it and the fact that more and more industries choose to deliver their offers as services. Good examples can be found in network services such as IPTV or IMS. The next two sections are geared towards presenting and demonstrating this innovation point.

2 Acknowledgement

The authors would like to thank Theo Dimitrakos, Head of the Security Architecture Group at BT Innovate, for his continuous contribution

3 References

[1] Dimitrakos, T., Brossard, D., de Leusse, P., “Securing Business Operation in SOA”, BT Technology Journal, vol.27, no.2, December 2008

[2] de Leusse, P., Periorellis, P., Watson, P. and Maierhofer, A, Secure & Rapid Composition of Infrastructure Services in the Cloud, In The Second International Conference on Sensor Technologies and Applications, SENSORCOMM 2008, 25-31 August 2008, Cap Esterel, France, IEEE Computer Society, 2008

[3] de Leusse, P., Periorellis, P., Watson, P. and Dimitrakos, T., A semi autonomic infrastructure to manage non functional properties of a service, In UK e-Science All Hands Meeting 2008, 8-11 September, Edinburgh, UK

[4] de Leusse, P., Periorellis, P., Dimitrakos, T. and Watson, P., An Architecture for Non Functional Properties Management in Distributed Computing, 3rd International Conference on Software and Data Technologies (ICSOFT 2008), 2008