RobustWeb: Development and Validation of SOA Applications based on *Web Services*

Eliane Martins[1], **Ana Cavalli**[2], **Jean Arlat**[3], **Regina Moraes**[1], **Taisy Weber**[4]

[1]Universidade Estadual de Campinas - UNICAMP
[2]TELECOM & Management SudParis
[3] LAAS-CNRS, Université de Toulouse
[4]Universidade Federal do Rio Grande do Sul - UFRGS

eliane@ic.unicamp.br, ana.cavalli@it-sudparis.eu, jean.arlat@laas.fr, regina@ceset.unicamp.br,taisy@inf.ufrgs.br

Abstract. *RobustWeb is a cooperation project joining Brazilian and French researchers to develop methods and tools that aim reaching Web Services robustness. The project encompasses seven institutions in both countries. All partners have long experience in the complete life cycle of software engineering, which constitute a solid basis to reach relevant results to face important challenges in the area of service-oriented architecture.*

1. Introduction

Service-orientation is an emerging paradigm for the development of distributed and e-business applications, in which the services (autonomous platform-independent computational elements that can be described, published, discovered and accessed over the Internet using standard protocols) are the new elements for development and reuse. This way of structuring an application in a set of interacting services is referred as Service-oriented Architectures (SOA).

In recent years, various approaches for implementing service-oriented architectures have appeared, and the majority of them uses Web Services (WS) as underlying technology for integration between different software applications. Web Service is a client-server system specially structured to make the best use as possible of Web standards, like XML for example. Today, different software vendors are launching their own solutions, as for instance Microsoft with .Net platform, Sun with Sun One initiative, and IBM with its WSDL tool kit development and execution environment. Web Services standards and their implementations are important to enable SOA wide acceptance. Various initiatives exist in that sense, such as the Web Services Interoperability Organization (WS-I), which is an open, industry organization committed to promoting interoperability among Web Services based on common, industry-accepted definitions and standards. Another one is the Organization for the Advancement of Structured Information Standards (OASIS), which defined a reference model for SOA.

These initiatives represent an essential step in the widespread adoption of WS and SOA in practice. However, composing a high quality SOA for the development of business or mission critical applications still stands at an early stage. The sources of failures for highly dynamic, distributed applications are innumerous. Besides, security aspects in this distributed, collaborative context are also an issue. In this respect, it is

important to provide guidelines on how to use the available techniques for the design of reliable architectures to compose their services. For some examples of relevant research efforts aimed at coping with these issues, see [Salatgé & Fabre 2007, Abou El Kalam & Deswarte 2008, Mallouli 2008]. Validation is another important aspect. The investigation of how to use testing techniques to the context of WS and SOA, as well as the modeling and evaluation of performance in this continually changing context will also be useful to guarantee that the desired level of quality is assured and maintained in spite of changes. Some of these issues are studied in the following works: [Cavalli 2007], [Mallouli 2008].

SOA-based architectures with Web Services are thus promising for the development of *omnivalent systems*, which are systems which present characteristics such as ubiquity, dependability and security. According to the document entitled *Grand Research Challenges in Computer Science in Brazil*, prepared in 2006 by the Brazilian Computer Society (www.sbc.org.br), these systems represent one of the research challenges nowadays. Developing and maintaining this kind of system represents a challenge in that combining the aforementioned properties is far from being easy. It has also been mentioned in [Laprie 2005], that dependability and security drop significantly for these emerging systems, compared with the traditional ones. On the other hand, the cost of failures in services is growing, given the increase in the presence of computer systems in everyone's lives. System development, and in particular SOA-based applications, has to deal with two main, sometimes contradictory, driving forces: increasing complexity and reduced time-to-market. Services reuse addresses the latter, but does not avoid the former. On the contrary, the complexity tends to increase, due to heterogeneity and the geographically distributed development and operation of Web Services based applications. These factors lead to more residual development defects, vulnerabilities and interaction mistakes, which represent threats to dependability and security of the applications [Laprie 2005].

The project *RobustWeb*, granted by CAPES/Cofecub, addresses this challenge. With this objective in mind, the project is aimed at covering the following issues presented by SBC:

- To integrate researchers into a multidisciplinary group that encompasses diverse research domains such as Dependability and Security Design and Validation, in this way covering not only the aspects relative to the construction of reliable and secure systems but also, those relative to the determination of whether the desired level of quality was achieved, which encompasses functional testing and robustness assessment activities, as well as performance evaluation and risk assessment.
- To promote meetings among the researchers, in one hand, to identify key research directions in the development and validation of reliable and secure SOA-based applications with Web Services. On the other hand, to organize workshops to help in propagate the best practices among practitioners and scientists.
- To increase the cooperation between Brazilian and French researchers, by bringing to Brazil visiting scholars that are active in the different domains covered by this project.

2. Partner institutions

The expertise needed to carry out the project is well covered by the gathered teams. All partners have long experience in the complete life cycle of software engineering: from fault-tolerant architectural modeling and formal specifications, to test specification and execution for applications, services and protocols. This includes timed aspects, automatic test generation, fault injection and building software engineering tools. More precisely, the main experience of each partner is:

- TELECOM & Management SudParis: methods and tools for test generation and monitoring, tool prototyping, Web Services technologies, web protocols and protocol architectures, engineering and standardization;
- LRI: random testing, statistical testing, modeling of Web Services; Web Services technologies including their standardization;
- LAAS-CNRS: analytical modeling and evaluation of fault tolerance, software testing, probabilistic generation of test data, fault injection, fault tolerance of web services, security.
- Unicamp: exception handling mechanisms; fault tolerance of concurrent and distributed object-oriented systems; dependable software architecture and component-based development; model-based testing; fault injection; methods and tools for building and testing dependable systems, risk assessment.
- II-UFRGS: developing of fault injection tools, communication fault injection, fault modeling of distributed systems, Internet protocols and their validation, fault tolerance in distributed systems, generation of fault loads for test campaigns.
- UFES: analytical modeling and evaluation of fault tolerance; performance evaluation of large scale distributed systems, Internet and web services measurements;
- INPE: model-based testing, methods and tools for test execution of embedded systems, tools for test execution and organizational aspects of test cases designed and executed along with the software development.

3. Project goals

The general objective of this project is to put together researchers in different areas, mainly: application architecture, security, testing and performance evaluation, to create guidelines and frameworks to assist service users and providers in the design and validation of services as well as the applications built by composing these services using the standards and technologies available for Web Services development and use.

The guidelines and frameworks been developing are based on best practices for software development, adapted to the context of WS and SOA. The intent is to help practitioners in the development of robust, fault-tolerant architectures, and that the services and applications implemented satisfy their functional requirements, but also present the required level of robustness, security and performance. The good practices help in reducing the costs as well as in increasing the productivity in the development or acquisition of services, as well as in their composition. More specifically, the intent is to provide a road map for the adoption of WS-based SOA to mission or business critical

applications. To illustrate the methods and techniques proposed, we are using as case study a space application from INPE, the Spacecraft Monitoring and Control (SM&C) system, which refers to end-to-end services between functions, resident on-board a spacecraft or based on the ground, that are responsible for mission operations.

The outcomes from the project will be knowledge, publications, training and technology transfer. In addition, the creation of new joint projects is also intended.

- Knowledge created by the project will be disseminated through conferences and journals.
- Education, training and technology transfer will also be sustained ways for disseminating and exploiting the results.
- Case studies are useful by themselves, as they are a springboard for realistic application of better network engineering and validation methods. By creating 'how to' guides based on case studies, the project will smooth the adoption of best network engineering and validation practices in industry.

4. Technical challenges

The project addresses important technical challenges [Martins 2008]. The first one is the design of an architecture that can maintain the desired level of reliability, availability and performance in the service composition, even when the services change at runtime and the only information about them is the specification of its public interface. Two approaches are possible. The first one defines how to use techniques to construct customizable fault-tolerant connectors to add fault-tolerance to unreliable WS [Salatgé & Fabre 2007]. These connectors insert detection actions (e.g. runtime assertions) and recovery mechanisms (based on various replications strategies). The connectors can use identical or equivalent available service replicas. The other approach adapts techniques for fault-tolerant composition of components, which are static, to the context of WS.

The next challenge is to adapt currently available model-based testing techniques for the testing of continually changing services and dynamic, loosely coupled applications to ensure that the composite services work properly. Two testing techniques will be investigated. One is active testing, in which test cases are generated from a model representing system behavior [Cavalli 2004]. We require new testing architectures that can take into account the tests executed remotely, with a minimum interference with the operation of the service being tested. Also, the dynamic changes of services must be considered. Another technique is based on passive testing, or monitoring, in which the traces collected during execution are used to determine whether a service behaves as expected. One important aspect from which guidelines are to be given concerns how to express these properties in a dynamically changing context.

Concerning test so far, the problem of testing the robustness of services without interfering with the normal operation of these services must also be solved. This challenge raises some issues related to managing the fault handler events, such as raising and handling of exceptions. Two approaches will be considered. One is property-oriented, which uses the specification of a property to drive the testing process. The aim is to exercise a system to observe whether the property is violated or not [Abdellatif-Kaddour 2003]. The properties of interest are any high level requirement

related to the most critical failure modes of the system. Another approach is fault injection that consists in the deliberate introduction of faults into a system to observe its behavior. Here also a model-based testing approach is to be investigated, the model representing either the architecture or the behavior of the service or the application. In case of behavior-based testing, the derivation of suitable models will be useful to fulfill this objective [Ambrosio 2005]. In case of an architectural model, the objective is to perform a dependency analysis to guide fault injection. In this way, we can assess the failure tolerance of the interfaces regarding component failures and corruptions that may enter into system from external sources [Moraes 2005].

How to evaluate the risk of using a service in a given application in a dynamic, constantly evolving context is another important challenge. The composition of the WS may come up with the choice among components that provide the same functionality. In order to guide the selection, a risk assessment can be performed. Previously, assessment of component risk was proposed, so that the component that represents lower risk to the overall system should be selected [Moraes 2007]. The approach was also based on fault injection, in which internal faults (representing faults occurring during development) were introduced into the component. It is necessary to adapt such approach to the WS-based SOA world, in which the services can change dynamically and should be tested sometimes remotely, with no interference with its operation.

The last challenge the project addresses is how to evaluate whether the desired level of performance is guaranteed in a dynamic, continually evolving context. The performance evaluation of web services involves traditional techniques which can be combined in a unified approach. In particular, our approach relies on the combination of analytical-based models and large scale experimental-based evaluation. From the application designers' point of view, it is critical to understand how different components of the distributed infrastructure supporting the provided service might affect the service. Based on the experimental results, analytical models will be built in order to support such analysis.

5. Conclusion

The project promotes opportunities of knowledge exchange among the partners. Most of these exchanges are been realized remotely, with the support of the Internet. In addition some project themes correspond to PhD thesis advised by the researchers in France and in Brazil. Doctoral as well as post-doctoral missions are envisaged between France and Brazil, encouraging the participation of the students in the project activities and stimulating their mobility.

Other planned project activities are the technical visits among the different institutions. These visits are aimed to consolidate the partnership and also to give rise to new collaborations. These researchers will present tutorials and talks to graduate students of the visited institutions, promoting therefore the transfer of knowledge.

References

Abdellatif-Kaddour, O.; Thévenod-Fosse, P.; Waeselynck, H. (2003). "A stepwise strategy for property-oriented testing", LAAS report no. 02351, September 2002. In Proc. 18th ACM Symposium on Applied Computing (SAC'2003), Melbourne, Florida, USA.

Abou El Kalam, A. and Deswarte, Y. (2008). "Critical Infrastructures Security Modeling,

Enforcement and Runtime Checking", in Proc. 3rd Int. Workshop on Critical Information Infrastructures Security (CRITIS 2008), Rome, Italy, pp.115-128.

Ambrosio, A.M.; Martins, E.; Vijaykumar N. L.; Carvalho, S.V. (2005). "A Methodology for Designing Fault Injection Experiments as an Addition to Communication Systems Conformance Testing," In Proc. of the First Workshop on Dependable Software – Tools and Methods in the IEEE Conference on Dependable System and Network, 28 June – 1 July 2005, Yokohama, Japan.

Cavalli ,A.; Maag, S.; Papagiannaki, S.; Vergiakis, G.; Zaïdi, F. (2004). "A Testing Methodology for an Open Software E-Learning Platform". In 18th IFIP World Computer Congress - TC10/WG10.5 Edutech Worskshop, pages 165-174, Toulouse, France. Kluwer Academic Publishers, ISBN 1-4020-8161.

Cavalli, Ana; Maag, Stephane; Morales, Gerardo (2007). "Regression and Performance Testing of an e-learning Web application: dotLRN". In 3rd ACM / IEEE International Conference on Signal-Image Technology and Internet-Based Systems (SITIS'07), Shangai, China.

Laprie, J.-C. (2005). "Resilience for the Scalability of Dependability". In Proceedings of the Fourth IEEE International Symposium on Network Computing and Applications (NCA'05). Cambridge, MA, USA.

Mallouli, Wissam; Lallali, Mounir, Morales, Gerardo; Cavalli, Ana (2008). "Modeling and Testing Secure Web-Based Systems: Application to an Industrial Case Study". In The Fourth ACM/IEEE International Conference on Signal Image Technology and Internet Based Systems SITIS '08, pages 128-136, Bali, Indonesia.

Martins, E. ; Moraes, R. ; Weber, T. S. ; Rubira, C. M. F. ; Ambrosio, A. M. ; Martinello, M. (2008). Desafios na construção e validação da robustez de aplicações orientadas a serviços. In Seminário Integrado de Software e Hardware, XXXV, Belém, pp. 62-76.

Moraes, R.; Martins, E.; (2005). "Fault Injection Approach based on Architectural Dependencies". Architecting Dependable Systems III, Book Chapter, Lecture Notes in Computer Science, Springer-Verlag Berlin Heidelberg New York, pp. 300-321.

Moraes, R.; Durães, J.; Barbosa, R.; Martins, E.; Madeira, H. (2007). "Experimental Risk Assessment and Comparison using Software Fault Injection". In The International Conference on Dependable Systems and Networks - DSN 07, Edimburgo.

Salatgé, N.; Fabre, J.-C. (2007) "Fault Tolerance Connectors for Unreliable Web Services". In 37th Annual IEEE/IFIP Int. Conf. on Dependable Systems and Networks (DSN-2007), Edinburgh, UK, pp.51-60.