On-line Validation of Service Oriented Systems in the European Project TAS

Antonia Bertolino, Guglielmo De Angelis
Istituto di Scienza e Tecnologie dell’Informazione “A. Faedo”
Consiglio Nazionale delle Ricerche – Pisa, Italy
{antonia.bertolino, guglielmo.deangelis}@isti.cnr.it
Andrea Polini
Department of Mathematics and Computer Science
University of Camerino – Italy
andrea.polini@unicam.it

Abstract

The European Project TAS addresses the challenge of combining the openness, flexibility, dynamicity offered by service-oriented applications, together with privacy, security and reliability characteristics that are required when personal information is handled. In addition to appropriate authorization and authentication mechanisms, it is important to put in place appropriate validation procedures that can check the trustworthiness and dependability of services provided. We outline the Audition framework and discuss how such on-line validation approach can fit within the TAS vision of a seamless connected world, where the final users remain in charge for releasing and administering their data.

1. Introduction

Whether we like it or not, the Internet has become an essential asset of our daily life. Being connected anytime anywhere brings positive and negative effects. Distance barriers are removed, and by virtual presence we can easily and effectively accomplish tasks that were not thinkable few years ago: shop without moving from our favorite armchair, attend a meeting at the other side of the world from our office, skip window queues to access our bank account. To achieve such advantages, the price to pay is to accept the increasingly intrusive presence of technology in our personal and business relations. Moreover, to permit the processing of business transactions such as those mentioned above, we need to consent the release of private and critical information (e.g., our credit card data, personal profiles, clinical records, ...) for transiting over the Internet at disposal of unknown people and software.

Therefore, so that openness, dynamicity and proactiveness offered by the Service-oriented Architecture (SOA) paradigm can be safely exploited, appropriate protection and certification mechanisms should be put in place to ensure that sensible data are properly used. For instance, when transactions are carried out on the internet, we cannot see who is on the other end, and therefore we need mechanisms to recognize who is actually the counterpart in a transaction, and if we can rely or not on them.

However, as the scale and pervasiveness of service networks handling massive distributed data grow, they become increasingly vulnerable. In modern service oriented systems trustworthiness intertwines technological and social aspects in many complex ways, and has probably become the most critical issue facing ICT researchers and developers. The adjective “trustworthy” comprehends: secure, reliable and resilient to attacks and operational failures; guaranteeing quality of service; protecting user data; ensuring privacy and providing usable and trusted tools to support the user in his security management. All such facets of trustworthiness need to be considered from the very outset of SOA development and integration, with societal and legal issues growingly impacting technological choices.

In this general context, we are currently investigating SOA validation from varying perspectives. In this position paper we report on issues encountered and on current research directions in testing services and service integrations in pervasive SOAs.

Testing is the prevailing industrial approach to validation, but also remains the activity that mostly impacts the development budget of software products. The dream of 100% testing automation is one of the pursued directions to face the growing quantity and complexity of software. The challenge is even tougher when the complexity of software meets the service-oriented paradigm. A SOA
lifecycle cannot be structured in well-defined development stages. Specifically, for a (composite) service it is not clear when testing starts or should end. A service usually relies on other external services which are developed and maintained by third-party providers. These external services may evolve or even change independently from the life-cycle of a service that is using them. Thus the execution environment for a service may evolve (and usually does) even after its deployment. Furthermore, it is also difficult to foresee the domain of all the possible users and user requests for a service.

The benefits with testing automation can be summarized in two simple points:

1. Repeatability of testing: testing activities are usually planned by development stages or releases, each testing activity can be replayed at each stage or release improving the efficiency and the efficacy of the test. Furthermore, there is the effective cost reduction of the testing infrastructure in long-term projects.

2. Increase the quality and the trust perceived by the users\(^1\) of the system

Thus, to achieve trustworthy SOA, there is the need to develop and use methodology and tools supporting the perpetual and automatic testing of software services. We have been active in such topic for some years. We have recently concluded the FP6 European Project PLASTIC [1], which released a platform enabling the development and deployment of robust distributed lightweight services in the B3G networking environment. In this PLASTIC platform, a validation framework has been included which supports offline and on-line validation of networked services regarding functional and extra-functional properties. Some of the PLASTIC results we achieved in SOA testing, are currently transferred and adapted to the ongoing FP7 European Project TAS\(^3\) [2]. As we summarise in the next section, TAS\(^3\) main focus is in the distributed service-oriented handling of person-related long-lasting information. In Sec. 3, we discuss the generic challenges of SOA testing and then in Sec. 4 we focus on the adaptation of Audition to TAS\(^3\) needs. Conclusions are briefly drawn in Sec. 5.

2. The TAS\(^3\) project vision

SOA is a very active research field. The development of “Pervasive and Trustworthy Network and Service Infrastructures” is a predominating theme of the seventh Framework Programme (FP7) of the European Community and several cooperative projects have been launched on this topic. Among these, the Integrated Project TAS\(^3\) (Trusted Architecture for Securely Shared Services) [2], started in 2008, specifically focuses on services centered around the management and treatment of personal information. The latter feature introduces special challenges to service developers and providers. Personal data are typically generated and evolved over a human lifetime. Such data are stored at distributed locations and used in a multitude of varying business processes.

TAS\(^3\) aims at providing a transparent framework in which services can securely process and depend on personal information. To this purpose TAS\(^3\) is developing a trusted architecture and set of adaptive security services which will preserve personal privacy and confidentiality in dynamic environments. It is clear that such an architecture is dependent on four very important requirements:

1. the personal information must be processed by service providers that are perceived to be trustworthy by the end users (the owners of the data) or by other service providers possibly involved;
2. all entities within the SOA that access and manipulate the personal information must be duly authorized to process this information;
3. all personal information should be managed and transferred securely;
4. cross-context processes must respect all relevant data protection requirements.

The goal of TAS\(^3\) is to demonstrate that its architecture can integrate in a generic and scalable way different technologies. End-users and service providers need to be authenticated and should prove their qualifications in a timely and revocable manner, through the use of credentials. End-users and service providers should be given mechanisms to specify which service providers they trust, and to provide trust and quality of service related feedback, so that this information can be used while executing the requested business processes. The disclosure of personal information throughout the complete architecture has to be constantly controlled, but also it must be made possible, temporarily and under precisely defined conditions, to overrule data protection policies using a “break the glass” or an “emergency override” procedure. Finally, transparency of business processes must be guaranteed throughout. Service requesters should have access to consult the transaction and audit trail of business processes that they initiated or in which their information was used.

Trustworthiness of TAS\(^3\) architecture, as above described, is clearly a very complex and articulated notion. In fact, the project intends to develop and integrate approaches for Identity management, Authentication and Authorization, security mechanisms to handle authorization and ac-

\(^1\)Here we mean as “users” either humans, or other software
cess control of workflows and their contexts, a dynamic infrastructure for management of credentials and policies, as well as a baseline of legal, privacy and ethics issues. A comprehensive definition of trust, as surveyed in [6], however, always includes a notion of reliability of the trusted party as perceived by the trusting party. A foundational aspect of reliability is proper functioning of the services, i.e., lack of failures and behaviour according to the specifications and published policies. Therefore, trust assessment must also be based on dynamic assessment [9]. TAS³ also includes plans for online testing of service compositions, that is under our responsibility.

3. SOA testing and trust

SOA characteristics outlined in the Introduction pose important challenges to activities related to the dynamic verification of service behaviour, inclusive of testing and runtime monitoring/analysis activities. Main objective of such activities is to check that the behaviour of the system, seen as a single service or as the integration of a set of services, is in accordance with the one expected.

In SOA, testing faces the following (non exhaustive) list of difficulties:

- Due to dynamic binding and context-dependency, it is not possible to know precisely before run-time the services with whom a given service will interoperate, and the assumptions made by such external services.

- The services composing a distributed SOA application are under the control of different organizations that tend not to disclose much about their operating environment; this reduces the possibility to access information that might be relevant for testing purposes.

- Even when the services with which a given service will interoperate are known, it may be impossible to run a distributed test checking their integration because the test invocations would not be distinguishable from real calls. This is particularly dangerous in case the test invocations use a stateful resource.

Rigorous dynamic verification is challenged by a completely open environment as the one prefigured by a pure SOA environment. Indeed, nowadays a common understanding is maturing among test researchers that the SOA paradigm can be better pursued within more controlled precincts. In particular, it is often assumed that the SOA infrastructure includes additional checking mechanisms and that service providers are willing to improve the verifiability of deployed services.

SOA also brings in some opportunities, among which we have previously investigated the usage of available formal or semiformal specifications, such as choreographies and orchestrations, for automatic test suites derivation.

Within the cited project PLASTIC [1], this has been combined with the exploitation of service registries as a new possible test agent, so deriving a new dynamic verification framework, called Audition [4]. The framework provides support to introduce a new testing phase to be carried on at deployment/publication time.

Indeed, registries are strategic within the SOA paradigm. Their main task is to provide references to existing services, thus allowing organizations unaware of each other to concretely interact. Trust on registries is a basic ingredient within any SOA infrastructure: a registry should behave fairly and provide service references without any direct interest. The Audition framework exploits further such reference role for registries, giving them the authority of deciding which services are accepted within a given SOA federation and which are not. As a result only “high quality” service references will be found within the service registry, resulting in increased trust on the other service participants and indirectly on the used SOA infrastructure.

4. Audition of Services within TAS³

As described above, TAS³ tackles how to securely share personal information among services interacting within a federated network of entities. Within a holistic approach for trust assessment, we propose to test remote services online and against the access policies they manifest. Our idea is to adopt and extend the Audition framework.

The role of the Audition registry could be performed under different methodologies. In the PLASTIC project, the decision was based on the execution of a test suite that assesses the conformance of the service to a defined specification. In the TAS³ architecture, we outline a possible scenario for such on-line testing infrastructure, in which, either event-driven or periodically, the TAS³ services are tested according to their declared policies. The role of the tester service is played by an extended service registry, to which we refer as the Audition Service Registry (ASR).

A service asks ASR for entering the TAS³ federation. It provides as usual the WSDL description of the exported interface. In addition, we assume it provides a model describing the access policy it claims to enforce. ASR tests the service under registration on-line and against its manifested policy. This stage is called Auditing [4].

During auditing, the ASR keeps working, but the service under registration is not index-linked into the directory service yet. The service under registration is marked to be in a pending-status.

The service registry validates the service under registration creating on-the-fly testers. Each tester invokes the service under registration playing one of the roles speci-
5. Conclusions

The overall aim of TAS3 is to research and develop a generic open and fully published trusted architecture for securely shared personal data services. This architecture will take into account all trust, security, identity management, privacy and dependability needs in order to gain a validated trust perception with the end-user.

This paper presents the approach to on-line validation that will be pursued within the TAS3 project. The approach starts from the consideration that a “pure SOA” infrastructure hinders verification-related activities. Within TAS3 we thus propose an audition phase to validate a service entering a TAS3 compliant infrastructure. The additional testing stage requires: the definition of expected service behaviour, and in particular its access policies, and the run-time support to verification. We believe such additional constraints could be accepted by service providers, in particular acting in federations within domains in which high levels of trust are required.

Acknowledgments This paper has been supported by the European Project FP7 IP 216287 TAS3.

References