City Research Online

City St George's, University of London

Citation: Anisetti, M., Ardagna, C. A., Guida, F., Gürgens, S., Lotz, V., Maña, A., Pandolfo, C., Pazzaglia, J., Pujol, G. & Spanoudakis, G. (2010). ASSERT4SOA: Toward Security Certification of Service-Oriented Applications. OTM Workshops, 6428 LNCS, pp. 38-40. doi: 10.1007/978-3-642-16961-8_11

This is the accepted version of the paper.

This version of the publication may differ from the final published version. To cite this item please consult the publisher's version.

Permanent repository link: https://openaccess.city.ac.uk/id/eprint/12614/

Link to published version: https://doi.org/10.1007/978-3-642-16961-8_11

Copyright and Reuse: Copyright and Moral Rights remain with the author(s) and/or copyright holders. Copies of full items can be used for personal research or study, educational, or not-for-profit purposes without prior permission or charge, unless otherwise indicated, provided that the authors, title and full bibliographic details are credited, a hyperlink and/or URL is given for the original metadata page and the content is not changed in any way. For full details of reuse please refer to City Research Online policy.

City Research Online: http://openaccess.city.ac.uk/ publications@citystgeorges.ac.uk

ASSERT4SOA: Toward Security Certification of Service-Oriented Applications

Marco Anisetti[1], Claudio A. Ardagna[1], Franco Guida[2], Sigrid Gürgens[3], Volkmar Lotz[4], Antonio Maña[5], Claudia Pandolfo[6], Jean-Christophe Pazzaglia[4], Gimena Pujol[5], George Spanoudakis[7]

[1] Università degli Studi di Milano, DTI, Crema, Italy
{claudio.ardagna,marco.anisetti}@unimi.it
[2] Fondazione Ugo Bordoni, Roma, Italy
guida@fub.it
[3] Fraunhofer Institute for Secure Information Technology, Germany
sigrid.guergens@sit.fraunhofer.de
[4] SAP Research, Sophia Antipolis, France
{jean-christophe.pazzaglia,volkmar.lotz}@sap.com
[5] University of Malaga, Computer Science Department, Malaga, Spain
{gimena,amg}@lcc.uma.es
[6] Engineering Ingegneria Informatica, Roma, Italy
claudia.pandolfo@eng.it
[7] City University London, Department of Computing, London, UK
G.Spanoudakis@soi.city.ac.uk

Abstract. ASSERT4SOA project proposes machine readable certificates to be used to allow Web service requesters to automatically assess the security properties of Web services (and their providers) as certified by some trusted third party. This vision promises to open up an entire new market for certification services.

1 Introduction

The term "certification" has been used with several different meanings in ICT [2]. Software practitioners can earn a certificate for expertise in a certain hardware or software technology. The maturity of crucial IT processes, such as software development, can be - and is often - certified. Even individual software systems can be certified as having particular non-functional properties, including safety, security, or privacy. The certification of non-functional properties, however, has had only a limited success to this day. Despite the availability of security certification schemes like Common Criteria [5] only a few commercial IT systems (e.g., those developed by highly regulated industries) have earned them.

In this paper we present the vision of ASSERT4SOA, a FP7 STREP project starting October 2010 that will deal with service certification issues. ASSERT4SOA, that builds over a number of research ideas put forward by consortium members [4], is aimed at supporting new certification scenarios, where the security certification of software systems is required and plays a major role.

Current trends in the IT industry suggest that software systems in the future will be very different from their counterparts today, due to greater adoption of Service-Oriented Architectures (SOAs), the wider spread of the deployment of Software-as-a-Service (SaaS), and the increased use of wireless and mobile technologies [6, 7]. These trends point to large-scale, heterogeneous ICT infrastructures hosting applications that are dynamically built from loosely-coupled, well-separated services, where key non-functional properties like security, privacy, and reliability will be of increased and critical importance.

In service-based scenarios, certifying software properties will be crucial. Current certification schemes, however, are either insufficient in addressing the needs of such scenarios or not applicable at all (e.g., certificate awarded to monolithic software systems only [1, 2]). ASSERT4SOA will fill this gap by producing novel techniques and tools for expressing, assessing, and certifying security properties for complex service-oriented applications, composed of distributed software services that may dynamically be selected, assembled, and replaced within complex and continuously evolving software ecosystems [3, 8].

2 ASSERT4SOA Certificates

ASSERT4SOA certifications will cover both individual software services and the environment in which they operate at execution time, allowing runtime management of the security, privacy and reliability properties, as well as business processes and applications based on them. ASSERT4SOA certificates will be handled by a dedicated set of newly developed services, collectively referred to as the "ASSERT4SOA architecture", fully integrated within the SOA-based software system lifecycle. The ASSERT4SOA architecture will enable: *i)* backward compatibility of existing certification processes within the SOA context; *ii)* a new ontology-based format for certificates, linking security properties with evidence supporting them; *iii)* runtime certificate-aware service selection based on target assurance level for composite applications.

ASSERT4SOA will support certificate-driven selection of individual services and, in addition, the evaluation of security properties of composites service based on the properties of their individual certified-services. The exploitation strategy of ASSERT4SOA certification scheme is threefold.

- To achieve the desired impact on the software certification community, ASSERT4SOA use cases will cover the whole SOA-based application lifecycle. Also, ASSERT4SOA will be providing methodological guidelines to support accredited certification agencies in the assessment of service-based composite applications.
- To reach out to SOA implementers, ASSERT4SOA will propose a standard ontology-based metadata format to express certified properties and will develop an architecture (components, protocols, and mechanisms) to use certification claims during the main phases of a service-based applications (e.g., deployment, lookup, service call, service composition).

– ASSERT4SOA will equip service-oriented application users with powerful, easy-to-understand mechanisms to assess at runtime the trustworthiness of composite applications. These mechanisms will use the security properties certified during the certification process of individual services; when a composite application will be orchestrated, the ASSERT4SOA infrastructure will compute the global level of assurance resulting from the interactions between the services in the given context.

These three exploitation objectives are incremental and aim to enable the progressive development of a new, service-based certification business ecosystems that will enable all European players - ranging from individual citizens to large businesses - to assess the security of the mission-critical applications they use based on a proven methodology.

3 Conclusions and Outlook

Early implementations of Web services tended to be sandbox-type services open to a small number of business partners with whom a trust relationship was already established. So the effort of understanding and assessing Web services' security properties was often perceived as superfluous. In recent years Web services have increasingly gained acceptance as the technology of choice for implementing inter-organizational business processes. In these situations, partners need additional information concerning the security schemes provided by each service to decide whether to use the service. The ASSERT4SOA vision proposes a machine readable certificate to be used to allow service requesters to assess the security properties of service providers as certified by some trusted third party. This vision promises to open up an entire new market for certification services.

References

1. A. Alvaro, E. de Almeida, and S. de Lemos Meira. Software component certification: A survey. In *Proc. of EUROMICRO 2005*, Porto, Portugal, August-September 2005.
2. E. Damiani, C. Ardagna, and N. El Ioini. *Open Source Security Certification.* Springer, 2009.
3. E. Damiani, N. El Ioini, A. Sillitti, and G. Succi. Ws-certificate. In *Proc. of the IEEE SERVICES I 2009*, Los Angeles, CA, USA, July 2009.
4. E. Damiani and A. Maña. Toward ws-certificate. In *Proc. of the ACM SWS 2009*, Chicago, IL, USA, November 2009.
5. D. Herrmann. *Using the Common Criteria for IT security evaluation.* Auerbach Publications, 2002.
6. M. Papazoglou, P. Traverso, S. Dustdar, and F. Leymann. Service-oriented computing: State of the art and research challenges. *Computer*, 40(11):38–45, 2007.
7. J. Robinson. *Demand for software-as-a-service still growing*, May 2009. `http://www.information-age.com/channels/commsand-networking/perspectives-and-trends/1046687/demand-forsoftwareasaservice-still-growing.thtml`, Accessed August 2010.
8. *Securing Web Services for Army SOA.* `http://www.sei.cmu.edu/solutions/softwaredev/securing-web-services.cfm`, Accessed August 2010.