



## AUTOMATED VALIDATION OF TRUST AND SECURITY OF SERVICE-ORIENTED ARCHITECTURES

LUCA VIGANO<sup>1</sup> (UNIVERSITY OF VERONA, ITALY)

**ABSTRACT.** The AVANTSSAR Project ([www.avantssar.eu](http://www.avantssar.eu)) has been developing an automated platform that provides a rigorous technology for the formal specification and Automated VALIDatioN of Trust and Security of Service-oriented ARChi- tectures. This technology, which is being tuned on a number of relevant industrial case studies so to allow for the migra- tion into the development process for software solutions for the Internet of Services, aims at speeding up the development of new network and service infrastructures, enhance their security and robustness, and increase the public acceptance of emerging IT systems and applications based on them. I will present the main techniques and technologies that are part of the AVANTSSAR Platform and some of the case studies it has been applied on. In particular, to illustrate the plat- form on the field, I will discuss our formal analysis of a SAML Web Browser Single Sign-On Protocol. Single-Sign-On (SSO) protocols enable companies to establish a federated environ- ment in which clients sign in the system once and yet are able to access to services offered by different companies. The Security Assertion Markup Language (SAML) Web Browser SSO Profile is the emerging standard in this context. We have provided formal models of the protocol corresponding to one of the most used use case scenarios (the SP-Initiated SSO with Redirect/POST Bindings) and of the implementa- tion used by SAML-based SSO for Google Applications. We have mechanically analyzed these formal models and thereby revealed a severe security flaw in the Google's implementa- tion that allows a dishonest service provider to impersonate a user and get unauthorized access to Google Applications (and viceversa). We have reproduced this attack in an actual deployment of the SAML-based SSO for Google Applications.