Putting a seal of security on the Internet of Services

September 12 2013

Credit: European Union 2013

Book a flight online, perform an internet banking transaction or make an appointment with your doctor and, in the not-too-distant future, the 'Internet of Services' (IoS) will come into play. A paradigm shift in the way ICT systems and applications are designed, implemented, deployed and consumed, IoS promises many opportunities but also throws up big challenges - not least ensuring security and privacy, issues currently being tackled by EU-funded researchers.

IoS is a vision of the future internet in which information, data and software applications - and the tools to develop them - are always accessible, whether locally stored on your own device, in the cloud, or arriving in real time from sensors. Whereas traditional software applications are designed largely to be used in isolation, IoS brings down

the barriers, thereby lowering costs and stimulating innovation.

Building on the success of cloud computing, IoS applications are built by composing services that are distributed over the network and aggregated and consumed at run-time in a demand-driven, flexible way. This new approach to software will make the development of applications and services easier - so that new and innovative services, not possible today, can be offered. It is likely to make a huge contribution to the EU's strategy to make Europe's software sector more competitive.

IoS services can be designed and implemented by producers, deployed by providers, aggregated by intermediaries and used by consumers. Anybody who wants to develop applications can use the resources in the Internet of Services to develop them, with little upfront investment and the possibility to build upon other people's efforts.

In many ways IoS solves the challenges of interoperability and inefficiency that can plague traditional software systems, but it can also create new vulnerabilities. How for instance can you trust that a service you are using is error free? Or that the different components from different developers that you are aggregating into a new application have all been tested for security vulnerabilities?

'Although it is always difficult to quantify exactly the impact of the absence of something, it is clear that the lack of efficient security validation technologies has been slowing down considerably the wide adoption of web services by citizens, many of whom still do not trust the internet in general nor the Internet of Services in particular,' warns Professor Luca Viganò at the Universita Degli Studi di Verona in Italy. 'It is thus not enough to develop good web-based services, nor to develop services that have been proved secure or which have been tested, but rather we also need a way to convince the citizen that they are indeed secure or have been thoroughly tested. The existence and use of

automated tools that can put their "seal of guarantee" on newly developed services, or on services that have been downloaded from the web, will certainly guarantee higher confidence and trust.'

Prof. Viganò and a team of researchers from five European countries are putting the finishing touches on tools to provide precisely that much-needed 'seal of guarantee' on web services. Their work, carried out in the 'Secure provision and consumption in the Internet of Services' (SPACIOS) project and supported by EUR 3.6 million in research funding from the European Commission, combines novel, state-of-the-art technologies for penetration security testing, vulnerability-driven security testing, mutation-based security testing, automatic learning for model inference, model checking and code extraction techniques.

A unique tool for security testing web services

'It is important to note that state-of-the-art security validation technologies exist, but they are typically used in isolation and at production time, whereas we need tools that can be employed to validate services at run-time,' Prof. Viganò explains. 'There are a number of other tools that have been used extremely proficiently for security testing, but none, to our knowledge, that combines all these techniques into one single tool, using one single formal language in input and output. The SPACIOS tool, we believe, possesses capabilities that no other tools exhibit.'

In grossly simplified terms, a user starts with a formal specification of the system to be tested in which its properties are specified as logical formulae. If no formal specification exists, the SPACIOS tool can generate a model automatically from the source code. The model is then tested for vulnerabilities using a state of the art model-checking platform called AVANTSSAR (that Prof. Viganò helped develop in a previous project).

If an attack is found, the model checker outputs an attack trace, which can be used to generate test cases for the system. If no attack is found, the model is mutated to force standard vulnerabilities in the specification and the tests are repeated. Any attack traces that are uncovered are used to generate test cases, which are then run against the system again. The process is repeated until all parameters and potential security vulnerabilities have been checked.

'It is important to note that the different components of the tool can be used separately, they are integrated into an Eclipse platform, which allows the user to choose what exactly they wish to do,' the SPACIOS coordinator says.

The team tested the tool in various industry-relevant application scenarios with real-world applications. They looked, for example, for security vulnerabilities in SAML 2.0 Web Single Sign-on (an emerging standard that enables online business partners to authenticate their users once within a federated identity environment) and in OpenID (an open and user-centric web-browser-based Single Sign-On protocol that provides a way to authenticate a user by asking them to prove that they control a unique identifier). Among other scenarios, they also applied the SPACIOS Tool to a set of open-source web applications that include an online bookstore, a site for classifieds and an employee directory. These web applications have previously been used as targets for both source code analysis and vulnerability testing.

Siemens and SAP, German industrial partners involved in SPACIOS, also put forward three other applications scenarios to validate the tool: Pervasive Retail (which contains a novel on-demand marketing management platform to create interactivity between consumers, retailers, and product providers through mobile phones), Infobase Document Repository (which implements a Document Management System that allows for the secure management and sharing of documents

or data files using web browsers) and eHealth (based on mash-up systems that on the one hand create and use electronic health records and on the other hand aggregate other functionalities, like decision support for the practitioner, analysis of images and billing systems).

Given the breadth of the Internet of Services and its likely rapid expansion over the coming years, the potential application scenarios for the SPACIOS tool are almost endless. Deployed widely, it would provide users with better security and lower web service development costs considerably.

'The SPACIOS approach will allow for smooth integration within the service development cycle, ranging from analysis at design time to testing at run-time, thus allowing developers to considerably reduce their costs. It is difficult to estimate this quantitatively, but we expect to be able to provide some measures once the integration has been taken up by the projects' industrial partners,' Prof. Viganò explains.

Though the partners have no immediate plans to directly commercialise the tool, it is already being used in industry by Siemens, SAP and others, Prof. Viganò says. The project partners are also discussing the possibility of a follow-up project to further enhance the fault and vulnerability testing technology.

SPACIOS received research funding under the European Union's Seventh Framework Programme (FP7).

Link to project on CORDIS:

- FP7 on CORDIS
- SPACIOS project factsheet on CORDIS

Provided by CORDIS