SPaCIoS

**Secure Provision and Consumption in the Internet of Services**

FP7-ICT-2009-5, ICT-2009.1.4 (Trustworthy ICT)

Project No. 257876

www.spacios.eu

---

# Deliverable D6.2.3

# Migration to industrial interest groups and open source communities


## Abstract

This deliverable discusses the migration experiences of SPaCIoS technologies to industrial interest groups (including standardisation bodies such as ETSI and OASIS) and open-source communities (e.g., OWASP, taking, in particular, advantage of our Expert Group, which comprises a representative of OWASP), including the release of mayor parts of the SPaCIoS toolset as open-source, made available to the general public for use and/or modification from its original design.


## Deliverable details


Deliverable version: *v1.0* Classification: *public*
Date of delivery: *07.10.13* Due on: *30.09.2013*
Editors: *Siemens, SAP and UNIVR principal editors; ETH Zurich, UNIGE, TUM secondary editors* Total pages: *25*


## Project details


Start date: *October 01, 2010* Duration: *36 months*
Project Coordinator: *Luca Viganò*
Partners: UNIVR, ETH Zurich, KIT/TUM, INP, UNIGE, SAP, Siemens, IeAT


---

SEVENTH FRAMEWORK PROGRAMME

# Contents

# 1 Introduction

This deliverable summarizes the migration experiences of SPaCIoS technologies to industrial interest groups (including standardisation bodies), and open-source communities.

In fact, the deliverable shows that the results of SPaCIoS have generated very successful input to industrial interest groups, including standardisation bodies (like ETSI, OASIS, and, indirectly, to the IETF), and open-source communities (like OpenSwan and OWASP). Also, the tools of the project are being offered as open source with an Eclipse license.

As part of our activities for the migration of project results to industrial interest groups, and in order to disseminate the project results in both the academic and the industrial communities, and plan further steps for dissemination, technology implementation, and exploitation, we organized a number of presentations and two *SPaCIoS Technology Migration workshops* in the summer of 2013, as well as the third meeting with the Expert Group of SPaCIoS. After discussing the migration to ETSI in Section 2, in Section 3.1.1, we describe SPaCIoS's participation to the OWASP's AppSec Research 2013 conference, organized by German OWASP Chapter in Hamburg on August 20-23, 2013. In Section 3.2.1, we describe the *Security Assessment for Systems, Services and Infrastructures workshop SASSI'13*, hosted by TU Berlin on September 19-20, 2013. SPaCIoS joined forces with the EU FP7 projects Diamonds, Intertrust, NESSoS and Rasen to organize this second "SPaCIoS Technology Migration workshop". In Section 3.2.2, we describe the main outcome of the third meeting with the Expert Group of the project, held in Berlin, Germany, on September 21, 2013, in conjunction with the SASSI'13 workshop.

In Section 4, we describe our activities in migrating project results to open source communities, in Section 5, we discuss the vulnerabilities found in standards and open source SW, and in Section 6 we draw some conclusions.

# 2 Migration to ETSI

ETSI, the European Telecommunications Standards Institute, is a major standardization organization with a strong industrial commitment and solid reputation for technical excellence. Its mission is to define globally-applicable standards for Information and Communications Technologies (ICT), including fixed, mobile, radio, converged, broadcast and internet technologies. It is officially recognized by the European Union as a European Standards Organization. ETSI is a not-for-profit organization with more than 700 ETSI member organizations drawn from 62 countries across 5 continents worldwide.

The ETSI Technical Committee on Methods for Testing and Specification (TC MTS) has created a work item "DTR/MTS-101582 SecTestCase" to discuss case study experiences related to security testing in order to have a common understanding in the TC MTS and related committees. Rapporteur is Juergen Grossmann from Fraunhofer FIRST, the Fraunhofer Institute for Computer Architecture and Software Technology, and Technical Officer is Emmanuelle Chaulot-Talmonfrom ETSI, France. The document covers industrial experiences from the following domains (in the current Version "DTS 201 582 V0.0.2" of Sept 2013): Banking (provided by DIAMONDS - Accurate Equity), Radio (provided by DIAMONDS - Thales), Automotive (provided by DIAMONDS - Dornier Consulting), e-Health (provided by SPaCIoS - Siemens), and Document Management and Sharing (Infobase, provided by SPaCIoS - Siemens). In the next future it may count with further case studies from the domains Smart Cards, Industrial Automation, Transport, Telecommunication or others.

The results were presented to ETSI MTS and discussed within the technical committee during the MTS SIG (Security Interest Group) Technical session on the 1st October 2013, 9am to 1pm. The results of SPaCIoS were very welcomed as they will help to clarify the security testing methodologies and the possible technologies that can be recommended, and even the terminology that should be adopted. This will be a long process, but the results of SPaCIoS have already a prominent place in the discussion.

# 3 Migration to OWASP and other industrial interest groups

As part of our activities for the migration of project results to industrial interest groups, and in order to disseminate the project results in both the academic and the industrial communities, and plan further steps for dissemination, technology implementation, and exploitation, we organized a number of presentations and two "SPaCIoS Technology Migration workshop" in the summer of 2013.

## 3.1 OWASP's AppSec Research 2013 conference and the First European workshop on Web Application Security Research (WASR'13)

### 3.1.1 OWASP's AppSec Research 2013 conference

First of all, several members of the SPaCIoS Consortium wrote the paper "A Tool for the Secure Provision and Consumption in the Internet of Services" [4], which was accepted in the research track of the AppSec Research 2013 conference, organized by German OWASP Chapter in Hamburg on August 20-23, 2013 (http://appsec.eu). The conference was attended by about 400 people from academia and industry, and was divided in several parallel tracks. The paper was presented by both Luca Compagna (SAP) and Luca Viganò (UNIVR) and the presentation included both a set of slides and a number of demos of the SPaCIoS Tool. This spurned quite some interest from the audience of our presentation, which comprised of about 100 people the vast majority of whom are involved in industrial research, with a small number coming from academia. Several of the attendees said that they will be interested in applying the SPaCIoS Tool once it is available in the spring of 2014.

The AppSec Research 2013 conference was attended by several members of the SPaCIoS project: Michele Peroli and Luca Viganò (UNIVR), Fabien Duchene and Karim Hossen (INP), Luca Compagna and Keqin Li (SAP), Petru Florin Mihancea (IeAT) and Martin Ochoa Ronderos (Siemens, TUM).

### 3.1.2 The WASR'13 workshop

In addition to participating to OWASP's AppSec Research 2013 conference, SPaCIoS joined forces with the EU FP7 projects WebSand, STREWS and NESSoS to organize the *First European workshop on Web Application Security Research* (WASR'13, https://appsec.eu/wasr/) hosted by the Ham-

burg University of Technology on August 19, 2013. This first "SPaCIoS Technology Migration workshop" was mainly invite-only, but a limited number of seats, and presentation slots, were open for participation from the public and people not part of the organizing projects.

**Workshop motivation** Since its birth in 1990, the Web has evolved from a simple, stateless delivery mechanism for static hypertext documents to a fully-edged run-time environment for distributed, multi-party applications. While this shift opens new opportunities — Business, Society, and Government rely more and more on the Web to provide their services to customers and citizens — it also increases significantly the complexity of the overall environment. The web technologies have gradually shifted from a central server technology towards a rich/stateful client paradigm and lively interaction models. The wave of popular peer-to-peer web applications and web mashup applications confirm this emerging trend. Users expect to use any of their devices to access on-demand applications to process resources stored somewhere else. But the shift from the server-centered paradigm poses a significant challenge of securing web applications in the presence of multiple stakeholders, including security-ignorant end-users. This motivates the need for solid "web application security" that shall target the overall cross-domains, cross-devices, and cross-services application together with the isolated components within it.

**Workshop format** This workshop is intended as a forum where recent research outcomes in the area of Web Application Security will be presented to security practitioners to get valuable feedback, trigger open discussions in the room, and promote outstanding EU-funded research. Presentations will cover topics, such as, protecting against pervasive threats (e.g., ClickJacking, XSS), security & Web standards, model-driven security testing, vulnerability-driven testing, mutation testing for security, Web application sandboxing, information flow security, attack detection and mitigation. The workshop will consist of a set of selected talks provided by the hosting projects as well as several invited presentations.

**Workshop program** The workshop was co-located with OWASP's AppSec Research 2013 conference, which allowed us to invite a number of conference participants and have a wide audience (of approximately 40 people). The workshop comprised of

- 25+5 minutes regular talks (including talks by Luca Compagna (SAP/

Cyspa & SAP/SPaCIoS), Johan Oudinet (TUM), Martin Ochoa Ronderos (Siemens, TUM) and Michele Peroli (UNIVR)),

- 10 minutes work-in-progress talks (including talks by Petru Florin Mihancea (IeAT), Karim Hossen (INP) and Fabien Duchene (INP)), and
- a panel "WebSec research meets the real world – what now?", with Luca Compagna (SAP/Cyspa & SAP/SPaCIoS) as panelist and Luca Viganò (UNIVR) as moderator.

and was structured according to the following program (where the talks by SPaCIoS researchers are highlighted in boldface):

| | |
|---|---|
| 08:30–08:50 | *Registration* |
| 08:50–09:00 | Opening remarks |
| 09:00–10:30 | Jonas Magazinius (Chalmers TH, WebSand): "Architectures for Inlining Security Monitors in Web Applications"<br>Thomas Roessler (W3C/STREWS): "On the ongoing standardization of Web & security and why you should care"<br>**Luca Compagna (SAP/Cyspa & SAP/SPaCIoS): "Instrumentation-based security testing"** |
| 10:30–11:00 | *break* |
| 11:00–13:00 | Konrad Rieck (University of Goettingen): "Learning-based Detection of Malicious JavaScript Code"<br>Sergio Maffeis (Imperial College London): "WebSpi: Discovering concrete attacks on security-sensitive web applications by formal analysis"<br>Ben Stock (FAU Erlangen/SAP Research/WebSand): "Eradicating DNS Rebinding with the Extended Same-Origin Policy"<br>Lieven Desmet (KU Leuven/STREWS/WebSand/ NESSoS): "Server-driven sandboxing of JavaScript" |
| 13:00–14:00 | *Lunch* |

| | |
|---|---|
| 14:00–15:30 | (Work in Progress session)<br>Bastian Braun (University of Passau/WebSand): "LogSec – A Smart Browser for Secure Web Sessions"<br>Willem De Groef (KU Leuven/WebSand/NESSoS): "Recent work on applications of SME on the server-side"<br>Johannes Dahse (Ruhr University Bochum): "Static detection of second-order vulnerabilities"<br>Sebastian Lekies (SAP/WebSand): "Large-scale Detection of DOM-based XSS"<br>**Petru Florin Mihancea (IeAT/SPaCIoS): "jModex: extracting models from web applications"**<br>**Karim Hossen (INP/SPaCIoS) "Model based testing without the pain of writing the model"**<br>**Fabien Duchene (INP/SPaCIoS) "KameleonFuzz: the day Darwin drove my XSS Fuzzer"** |
| 15:30–16:00 | *break* |
| 16:00–17:30 | **Johan Oudinet (TUM/SPaCIoS): "SPaCiTE: a mutation-based security testing tool"**<br>**Martin Ochoa Ronderos (Siemens, TUM/SPaCIoS) & Michele Peroli (UNIVR/SPaCIoS): "VERA: a vulnerability-driven security testing tool"**<br>Mario Heiderich (RUB/Cure53): "JSMVCOMFG – To sternly look at JS MVC and Templating Frameworks" |
| 17:30–18:15 | **Closing panel: "WebSec research meets the real world – what now?"**<br>Panelists: Boris Hemkemeier (Commerzbank), Jim Manico (White Hat Security), **Luca Compagna (SAP/Cyspa & SAP/SPaCIoS)**, Joachim Posegga (Uni Passau)<br>**Moderation: Luca Viganò (UNIVR/SPaCIoS)** |

The talks by Luca Compagna (SAP) and Luca Viganò (UNIVR), Johan Oudinet (TUM), Martin Ochoa Ronderos (Siemens/TUM) and Michele Peroli (UNIVR), Petru Florin Mihancea (IeAT), Karim Hossen (INP), and Fabien Duchene (INP) included both slides and demos of the different components of the SPaCIoS Tool and were received with much interest by the audience. In general, the workshop was, we believe, a great success, up to the point that we are planning a second one for 2014, although the constituent projects will be completed by then.

## 3.2 The Security Assessment for Systems, Services and Infrastructures workshop (SASSI'13) and the third meeting with the Expert Group of SPaCIoS

### 3.2.1 The SASSI'13 workshop

SPaCIoS joined forces with the EU FP7 projects Diamonds, Intertrust, NESSoS and Rasen to organize the *Security Assessment for Systems, Services and Infrastructures workshop* (SASSI'13, http://de.amiando.com/SASSI13.html) hosted by TU Berlin on September 19-20, 2013. This second "SPaCIoS Technology Migration workshop" was again mainly invite-only, but some presentation slots were open for people not part of the organizing projects.

**Workshop motivation** Security failures and data breaches are impacting not only enterprises but also critical infrastructures and public services. Solely in Germany successful attacks on IT systems in cause damage by 4.8 million Euros a year. At the same time, we are experiencing how the current IT landscape is changing rapidly. Just a few years ago, the Internet was dedicated to interconnect stationary end user devices.

Nowadays, the tendency towards an Internet of things makes the situation more complex. Mobile devices, home automation, smart grids and even vehicles are connected via the Internet and becoming theoretical accessible and thus vulnerable to hacker attacks. However, we are more than ever dependent on a secure and mature ICT infrastructure. One of the keys to get and maintain such a secure and dependable infrastructure is a mature, systematic and capable security risk analysis and testing program.

**Workshop format** The workshop will provide a forum to discuss innovative security testing approaches and their combination with security risk analysis. At the same time, the workshop tries to draw a line to the industrial requirements and the challenges that arise when security testing meets the demands of cost efficiency and scalability. Experts from industry and academia will present and discuss their solutions to the key issues security risk analysis, vulnerability testing, model based security testing, and standardization. The contributions are complemented by industry grade research results from four large European research projects.

**Workshop program** The SASSI workshop was attended by approximately 40 people (from the organizing projects, academia or industry), including 11 members of the SPaCIoS consortium and the 3 members of the Expert Group

(namely, Matteo Meucci, Sachar Paulus, Alexandre Petrenko), who we invited to attend (Sachar Paulus also gave a talk about his own work). The workshop was structured according to the following program (where the talks by SPaCIoS researchers are highlighted in boldface):

**Day 1, September 19**

| | |
|---|---|
| 10:00–10:45 | Keynote: *Cyber security*<br>Ralf Böker, Federal Office for Information Security (BSI) |
| 10:45–11:30 | Keynote: *Risk analysis and testing - perspectives from the frontline*<br>Stig Torsbakken (Nets) |
| 11:30–13:00 | *Session 1: Security risk assessment and testing*<br>**Jorge Cuellar and Jan Stijohann (Siemens): Siemens, Risk-based testing**<br>Ketil Stolen (SINTEF): Test-based risk assessment<br>Samson Yoseph Esayas (University of Oslo): Legal Risk Management: a Method for Proactive Management of Legal Risks |
| 13:00–14:00 | *Lunch* |
| 14:00–16:30 | *Session 2: Standardization & Certification*<br>Gerard Gaudin ($G^2$2C, France): A full set of new standards in Cyber Defence addressing the full scope of security event detection issues<br>Jürgen Großmann Fraunhofer FOKUS: Security Testing Improvement Profile (STIP)<br>**Luca Viganò (Università di Verona, Italy): The SPaCIoS Tool - property-driven and vulnerability-driven security testing**<br>**Luca Compagna (SAP): Formal Validation and Testing of Security Standards at SAP, from research to industry** |
| 18:30– | *Social event* |

**Day 2, September 20**

10:00–12:00 *Session 3: Active security testing*
Bruno Legeard (FEMTO-ST/UFC & Smartesting): Model-based vulnerability testing from patterns and behavioral model
**Martín Ochoa (Siemens/TUM): Model-based vulnerability testing**
Sachar Paulus (Kuppinger Cole): Trustworthy software development
Ari Takanan (Codenomicon): Traffic Capture Fuzzer: Effective method for model based fuzzing

12:00–13:00 *Lunch*

13:00–16:00 *Session 4: Active and passive security testing*
Riccardo Scandariato (KULeuven): Security vulnerability prediction
Graham Steel (Cryptosense, Paris): Security analysis of APIs, including the W3C Crypto API
Ana Cavalli (Institut Mines-Telecom, France): Application of passive testing techniques to secure interoperability testing
Wissam Mallouli (Montimage): Passive testing for security checking using MMT

The talks by Jorge Cuellar and Jan Stijohann (Siemens), Luca Viganò (UNIVR), Luca Compagna (SAP) and Martin Ochoa Ronderos (Siemens and TUM) included both slides and demos of the different components of the SPaCIoS Tool and were received with much interest by the audience. We believe that also this workshop was a success and also in this case we are planning a second one for 2014, although the constituent projects will be completed by then.

In addition to the speakers, the workshop was attended by the following members of SPaCIoS:

- Davide Guardini (UNIVR),
- Michele Peroli (UNIVR),
- Grgur Petric Maretic (ETH Zurich),
- Roland Groz (INP),
- Jean-Luc Richier (INP),
- Gabriele Costa (UNIGE),

- Luca Compagna (SAP),
- Jorge Cuellar (Siemens),
- Marius Minea (IeAT),
- Martin Ochoa (Siemens/TUM).

All these SPaCIoS members (except for Luca Compagna of SAP, but with the participation of Keqin Li of SAP via remote connection) also participated to a general project meeting, held on September 18, 2013, and to the meeting with the Expert Group of SPaCIoS, held on September 21, 2013.

### 3.2.2 The Third Meeting with the Expert Group of SPaCIoS

In this section, we describe the main outcome of the third and final meeting with the Expert Group, which was held in Berlin, Germany, on September 21, 2013, in conjunction with the SASSI'13 workshop.[1]

The Expert Group comprised:

- Matteo Meucci: Chair of the Italian Chapter of OWASP, leader of the OWASP Testing Guide, and CEO of an SME ("Minded Security") actively working in security represents security practitioners/analysts.
- Sachar Paulus: Senior Analyst at Kuppinger Cole, CEO of a management consultancy for security ("paulus.consult"), and member of a number of advisory boards (e.g., RISEPTIS, the Advisory Board for Research and Innovation on Security, Privacy and Trust in the Information Society), represents security analysts and advisors.
- Alexandre Petrenko: Team Director Distributed Systems Analysis at CRIM (a non-profit organization) leads various projects focused on technology transfer to industry in the area of testing framework, methodology, and tools targeting functional and security aspects of IT systems, and thus represents testing experts and technology transfer specialists.

The SPaCIoS consortium was represented by:

- Davide Guardini (UNIVR),
- Michele Peroli (UNIVR),
- Luca Viganò (UNIVR),

[1] This description already includes the comments that we received from the Expert Group.

- David Basin (ETH Zurich),
- Grgur Petric Maretic (ETH Zurich),
- Roland Groz (INP),
- Jean-Luc Richier (INP),
- Gabriele Costa (UNIGE),
- Luca Compagna (SAP),
- Jorge Cuellar (Siemens),
- Marius Minea (IeAT),
- Martin Ochoa Ronderos (Siemens/TUM).

The SPaCIoS consortium sent to the Expect Group both the project documents already delivered in period P3 (D1.3 [15], D2.2.1 [20], D2.2.2 [21], D2.4.1 [16], D2.5.1 [22], D3.3 [23], D3.5 [24], D4.2 [17], D5.2 [18], D5.3 [25], D6.1.3 [19], D6.2.2 [26], as well as the new DoW amended to consider the 4-month project extension) and a summary of the main deliverables due at month 36.

Following the Description of work, the meeting lasted one day and was structured along a number of general sessions devised to provide input to the Expert Group by summarizing the progress of the project and illustrating the next steps, and to capitalize on the expert's vision on new activities and technologies, enabling the consortium to track and make use of the state-of-the-art in terms of industrial practices and standards, and thereby allow for a wider take up of the project's foreground. In addition to the SPaCIoS presentations by Luca Viganò, Luca Compagna, Jorge Cuellar and Martín Ochoa at the SASSI'13 workshop, the meeting was organized so as to present and demonstrate the different components of the SPaCIoS Tool and was thus structured according to the following agenda (which slightly deviates from the one in the DoW in order to be able to tell a coherent and more poignant story in this final meeting):

**9:00—10:30** (SPaCIoS → Expert Group)

- Overview of the meeting, and of the last 12 months and the 4 month project extension (presentation by UNIVR).
- The SPaCIoS Tool (presentation by UNIGE).

- jModex: attack discovery using models extracted from source code (presentation by IeAT).
- LTL separation and the SAML case study (presentation by ETH Zurich).

**10:30—11:00** Coffee break

**11:00—12:30** (SPaCIoS → Expert Group)

- KameleonFuzz: fuzzing for XSS (presentation by INP).
- Information Flow (presentation by Siemens and TUM).
- Spacite and Vera (presentation by TUM).
- Instrumentation-based testing (presentation by SAP).
- Industry migration to Siemens and Migration to industrial interest groups and open source communities (presentation by Siemens).
- Dissemination and exploitation actions and plans, and Life after SPaCIoS (presentation by UNIVR).

**12:30—13:15** Lunch

**11:00—12:30** Expert Group meets in private

**11:00—12:30** (SPaCIoS ← Expert Group)

- Feedback and closure of the meeting

The meeting was very productive and the Expert Group provided comments and feedback that are both stimulating and challenging for the project. After a quick meeting in private, the Expert Group provided us with the following feedback:

> We enjoyed this day, and the SASSI 13 workshop, very much; we observed a very good progress on a number of things, not just theoretical presentations but also tool demos. We have a number of suggestions for the final months of the project and for the dissemination and exploitation of the project results in the future:
>
> 1. Strengthen the scientific output of the project through additional publications and workshops. Consider setting up an internal quality assurance process to improve the acceptance rate of papers submitted out of the project, especially for the less visible project results.

2. Deploy the tools from the project in more community platforms: NESSOS, Polarsys, FI-PPP (components that may serve as a generic enabler); donate (some) tools to OWASP.
3. Develop a "final presentation" that can be used by every project partner. It should not only describe the tool, but also emphasize a big picture how the different technologies work together, and demonstrate the overall value of the results.
4. Describe usage scenarios and, if applicable, conditions where the tool(s) can demonstrate the effect of reducing the overall testing efforts. This could be used in the "final presentation" and other project deliverables.
5. Regarding the life after the project end, consider submitting a project proposal that covers less addressed topic areas (such as, e.g., time constraints, business application logic).

The meeting was concluded by a quick summary of the main issues discussed and by a plan of the steps that will take into account the feedback of the Expert Group and lead to the conclusion and afterlife of the SPaCIoS project.

# 4 Migration to Open Source Communities

## 4.1 VERA

The VERA component will be released as open source under the Eclipse Public License (EPL) 1.0. It will be made available together with the other components of the SPaCIoS and will include the following:

- A set of Eclipse plug-ins created to design and run low-level attacker models.
- An autonomous VERA back-end command-line interface.
- A VERA plug-in for the Burp Suite Pro vulnerability scanner.
- A set of low level attacker models and instantiation libraries.

## 4.2 SIMPA

The model inference tool *SIMPA* developed by Grenoble INP will be released as an open source software under the Eclipse Public License (EPL) 1.0. This tool will be provided as a component of the SPaCIoS tool and it is divided in the following Eclipse plug-ins:

- A set of Eclipse plug-ins for the integration in Eclipse.
- A standalone version of *SIMPA* available through command-line interface and from Eclipse.
- A standalone test driver generator also integrated in *SIMPA*.
- A set of examples including test drivers and models.

## 4.3 Instrumentation Based Security Testing Tool

The "Instrumentation Based Security Testing Tool" developed by SAP has passed SAP's internal approval procedure, and will be provided as open source under Eclipse Public License (EPL) 1.0. It will be hosted together with other components of the SPaCIoS Tool. It contains a group of Eclipse plug-ins, whose main functions include:

- Syntax highlighting of ASLan++.
- Automatic translation of ASLan++ to ASLan by invoking the "ASLAN++ Connector", which is available as open source under Apache 2.0 license.

- Invoking SATMC, which must be downloaded by the users separately.
- Visualizing the output of model checker as a message sequence chart.
- Facilitating the definition of System Under Test (SUT), i.e., defining the mapping between formal specification elements and concrete software artifacts.
- Facilitating the definition of adapters, which are needed in order to execute security tests on an SUT.
- Executing the output of model checker as security test on a defined SUT.

## 4.4 SPaCiTE

SPaCiTE was developed by TUM and will be distributed in two different versions. As part of the SPaCIoS Tool, we will distribute a "Pro" version in binary form. In addition, we will provide a "Basic" version as open source under Eclipse Public License (EPL) 1.0. It will be hosted together with other components of the SPaCIoS Tool. The "Pro" version will be provided on request. Both versions of SPaCiTE consist of the following sub modules:

- ASLan++ Mutation Tool.
- ASLan++2WAAL translator to map abstract attack traces as a sequence of messages to a sequence of browser actions.
- WAAL2JAVA translator to translate test cases expressed in the WAAL language to executable test cases in Java.
- Test Execution Engine to execute concrete test cases.
- ControlProxy to control WebScarab and the Selenium Server.

The "Pro" and the "Basic" versions only differ in the number of provided mutation operators in the ASLan++ Mutation Tool.

## 4.5 jModex

The model extraction tool jModex developed by IeAT will be released as an open source software under the MIT license. The tool will be deployed as a component of the SPaCIoS tool providing the feature of automatic extraction of ASLan++ models for a system under test by analyzing the application

code. Various configuration options can be set by the user (via a dedicated property view) including:

- Selection of technology-specific abstractions and their configuration (e.g., providing the file containing the database structure).
- Adding into the analysis supplementary abstractions defined programmatically by the JMODEX user.
- The location of the resulting model.

## 4.6 Contribution to open platforms

The NESSoS Service Development Environment (SDE) is an open, Eclipse-based platform for the development of web services. Its structure has been defined in the scope of the NESSoS project [10] in order to collect technologies provided by different contributors. In this respect, every tool developed in SPaCIoS can be easily ported to the NESSoS platform. The main advantage of this technological migration is a considerable improvement of both the usability and visibility of the SPaCIoS approach.

For the time being, two components of the SPaCIoS Tool have been made compatible with the NESSoS SDE, i.e., JMODEX and SATMC. In particular, they have been extended with interface implementations for interacting with the orchestration environment provided by the NESSoS SDE. The orchestrator allows developers to easily compose, even graphically, technologies in a single service object. Moreover, new entries have been added to the NESSoS Common Body of Knowledge (CBK) in order to augment their visibility within the NESSoS user community.

Although the NESSoS SDE is just one instance of open platform, it relies on standard integration, i.e., based on plug-ins, procedures. Hence, we expect the same approach to apply to other Eclipse-based platforms.

# 5 Vulnerabilities found in Standards and in Open Source SW

## 5.1 OpenSwan

As part of a project on fuzz-testing of security protocols, we tested the open-source software OpenSwan [14] for vulnerabilities, and collaborated with OpenSwan's developers to fix several previously unknown vulnerabilities that we discovered. OpenSwan is a mature implementation of the Internet Key Exchange protocol (IKE) [8, 9]. The software is widely used for setting up secure communication channels within numerous Linux distributions.

We used SecFuzz [28] to fuzz-test OpenSwan's latest version for security vulnerabilities. To check whether we have thoroughly tested the software, we measured the coverage of the tests using the semi-valid input coverage criterion [29]. We discovered three previously unknown vulnerabilities in OpenSwan. All vulnerabilities have been privately reported to OpenSwan's developers. In the following, we report on the vulnerabilities and our collaboration with the developers.

We first discovered a use-after-free vulnerability [6]. To pinpoint the fault we manually inspected OpenSwan's source code. We found that when OpenSwan exchanges a shared key with another endpoint, it spawns a *crypto helper* thread to compute the shared key. OpenSwan passes to this thread a pointer to a data structure that contains the information for computing the key. We noticed that OpenSwan frees the data structure when the connection between the endpoints is closed, which can be triggered by sending a close session message to OpenSwan. This introduces a data race: if the connection between the endpoints is closed before the crypto helper thread has terminated, the thread accesses freed memory. This vulnerability may cause OpenSwan to crash, use unexpected values, or execute malicious code. Note that OpenSwan runs with administrator privileges, and an attacker may exploit the vulnerability to escalate her privileges.

We reported the vulnerability to OpenSwan's developers. We helped the developers in reproducing the vulnerability and they proposed two patches to fix the problem. We then tested the patched OpenSwan versions for vulnerabilities and discarded one of them because we found a denial-of-service vulnerability in it. The other patch successfully fixes the use-after-free vulnerability. The patch was released to the public and the major Linux distributions posted details about the vulnerability and the security patch on their security bulletins [1, 27]. More details on the vulnerability and the patch are given in CVE-2011-4073 [6].

The other two vulnerabilities that we discovered are an access of unallocated memory [5] and an access of uninitialized memory [7]. The underlying cause for both vulnerabilities is OpenSwan's improper checking of messages for missing fields. More specifically, the first message received by OpenSwan contains an identifier of the endpoint that initiates the protocol. IKE defines different identifier types such as IPv4, IPv6, and X.501 distinguished names. We found that for some identifier types OpenSwan does not check whether the identifier field is contained in the message. A vulnerability is exposed when OpenSwan receives a message with an IPv6 identifier, but the field storing the IPv6 address is omitted in the message. OpenSwan does not check the length of the message and accesses unallocated memory [5]. This vulnerability may be used to crash the program or to execute arbitrary code. A similar vulnerability is exposed when OpenSwan receives a message with an X.501 distinguish name identifier. If the identifier field is omitted, OpenSwan accesses uninitialized memory [7]. An attacker may exploit such a vulnerability to crash the program and, depending on the memory layout, to execute arbitrary code.

Both vulnerabilities have been reported to the OpenSwan's developers. To help the developers to reproduce the vulnerabilities and debug OpenSwan, we gave them the concrete IKE messages that expose the vulnerabilities and the corresponding stack traces of the memory violations.

## 5.2 SAML

SAML was from the beginning one of the proposed use cases for our project. A more technical description of the work of SPaCIoS on SAML has been presented in several other deliverables, including D2.2.1 [20], D2.4.1 [16], D2.5.1 [22], D5.2 [18], D5.3 [25], and D6.2.2 [26].

The two major contributions to the SAML standard are

- the discovery of an authentication flaw that allows a malicious service provider to hijack a client authentication attempt or force the latter to access a resource without its consent or intention. This may have serious consequences, as evidenced by a Cross-Site Scripting attack that we have identified in the SAML-based SSO version for Google Apps and in implementations of the SSO standard, including the one available in Novell Access Manager v.3.1. For instance, the attack allowed a malicious web server to impersonate a user on any Google application. We have also described solutions that can be used to mitigate and even solve the problem. These problems and the corresponding proposals for solutions have been discussed in the journal article in Computers &

Security [3] and in the IFIP TC Conference [2].

The OASIS Security Services (SAML) Technical Committee has welcomed the input from SPaCIoS and has approved the Errata 05 of SAML Version 2.0 the 1st of May 2012, [13]. Section "E90: RelayState sanitization" modifies the specifications "SAML Bindings" [11] and "SAML Profile" [12] in several ways. The errata acknowledges the EU Projects AVANTSSAR, SPaCIoS, and SIAM for the identification of the problem, and assistance in drafting the material.

- SAML problems related to an XML Signature Wrapping Attack, which are described in detail in D2.4.1 [16], and D2.5.1 [22].

# 6 Conclusions

The results of SPaCIoS have been very successfully brought to industrial interest groups, including standardisation bodies, like ETSI, OASIS, and, indirectly, to the IETF, and to open-source communities like OpenSwan and OWASP. Also, the tools of the project are being offered as open source with an Eclipse license.

From the start, SPaCIoS demonstrated its drive in presenting its results to industrial interest groups, standardisation bodies, and open-source communities, in order to achieve a profound and long-lasting impact. The three general avenues of migration to industrial interest groups and open-source communities have been:

- The SPaCIoS Toolset was successfully used to discover attacks that affected standards and implementations of standardisation bodies and open-source communities. The team members thoroughly discussed with the respective organization the details of our findings and helped updating the standard or implementation affected.
- The project also provided input to ETSI, the standardisation body in charge of creating testing standards related to the communication technology. Our goal is to provide experiences on the testing methodology applied to concrete use cases, which may help in the formulation of new standards or of its application recommendations.
- We organized a number of presentations and two *SPaCIoS Technology Migration workshops* in the summer of 2013, as well as the third meeting with the Expert Group of SPaCIoS.

# References

[1] Debian Security Advisory. DSA-2374-1 Openswan - Implementation Error. http://www.debian.org/security/2011/dsa-2374.en.html.

[2] Alessandro Armando, Roberto Carbone, Luca Compagna, Jorge Cuellar, Giancarlo Pellegrino, and Alessandro Sorniotti. From Multiple Credentials to Browser-based Single Sign-On: Are We More Secure? In J. Camenisch, S.F.H. Bner, S. Fischer-Hübner, Y. Murayama, A. Portmann, and C. Rieder, editors, *Future Challenges in Security and Privacy for Academia and Industry: 26th IFIP TC 11 International Information Security Conference, SEC 2011, Lucerne, Switzerland, June 7-9, 2011, Proceedings*, IFIP Advances in Information and Communication Technology Series, pages 68–79. Springer, 2011.

[3] Alessandro Armando, Roberto Carbone, Luca Compagna, Jorge Cuellar, Giancarlo Pellegrino, and Alessandro Sorniotti. An authentication flaw in browser-based single sign-on protocols: Impact and remediations. *Computers & Security*, 2012.

[4] The SPaCIoS Project Consortium. A Tool for the Secure Provision and Consumption in the Internet of Services. In *OWASP AppSec Research 2013*. https://appsec.eu, 2013.

[5] The MITRE Corporation. CWE-120: Buffer Copy without Checking Size of Input. http://cwe.mitre.org/data/definitions/120.html, October 2008.

[6] The MITRE Corporation. CWE-416: Use After Free. http://cwe.mitre.org/data/definitions/416.html, September 2011.

[7] The MITRE Corporation. CWE-824: Access of Uninitialized Pointer. http://cwe.mitre.org/data/definitions/824.html, May 2012.

[8] D. Harkins and D. Carrel. The Internet Key Exchange (IKE). RFC 2409 (Proposed Standard), November 1998. Obsoleted by RFC 4306, updated by RFC 4109.

[9] D. Maughan, M. Schertler, M. Schneider, and J. Turner. Internet Security Association and Key Management Protocol (ISAKMP). RFC 2408 (Proposed Standard), November 1998. Obsoleted by RFC 4306.

[10] NESSOS: Network of Excellence on Engineering Secure Future Internet Software Services and Systems. www.nessos-project.eu, 2010.

[11] OASIS. Bindings for the OASIS Security Assertion Markup Language (SAML) V2.0. http://docs.oasis-open.org/security/saml/v2.0/samlbindings-2.0-os.pdf, March 2005.

[12] OASIS. Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0. http://docs.oasis-open.org/security/saml/v2.0/samlprofiles-2.0-os.pdf, March 2005.

[13] OASIS. SAML V2.0 Errata, May 2012. Available at: http://docs.oasis-open.org/security/saml/v2.0/errata05/os/saml-v2.0-errata05-os.html.

[14] OpenSwan. https://www.openswan.org/projects/openswan/.

[15] SPaCIoS. Deliverable 1.3: Periodic Progress Report for Period 2, 2012.

[16] SPaCIoS. Deliverable 2.4.1: Definition of Attacker Behavior Models, 2012.

[17] SPaCIoS. Deliverable 4.2: SPaCIoS Tool v.1 and Validation methodology patterns (final version), 2012.

[18] SPaCIoS. Deliverable 5.2: Proof of Concept and Tool Assessment v.2, 2012.

[19] SPaCIoS. Deliverable 6.1.3: Dissemination and Exploitation Plan v.2, 2012.

[20] SPaCIoS. Deliverable 2.2.1: Method for assessing and retrieving models, 2013.

[21] SPaCIoS. Deliverable 2.2.2: Combined black-box and white-box model inference, 2013.

[22] SPaCIoS. Deliverable 2.5.1: Framework for Concretisation of Abstract Tests, 2013.

[23] SPaCIoS. Deliverable 3.3: SPaCIoS Methodology and technology for vulnerability-driven security testing, 2013.

[24] SPaCIoS. Deliverable 3.5: Methodology for fault localization based on execution traces, 2013.

[25] SPaCIoS. Deliverable 5.3: Final Proof of Concept, 2013.

[26] SPaCIoS. Deliverable 6.2.2: Migration to SAP and SIEMENS business units (lessons learned and best-practices), 2013.

[27] Red Hat Security Response Team. CVE-2011-4073. https://access.redhat.com/security/cve/CVE-2011-4073/.

[28] Petar Tsankov, Mohammad Torabi Dashti, and David Basin. SecFuzz: Fuzz-testing Security Protocols. In *Proceedings of the 7th International Workshop on Automation of Software Test*, AST'12, pages 1–7. ACM, June 2012.

[29] Petar Tsankov, Mohammad Torabi Dashti, and David Basin. Semi-valid Input Coverage for Fuzz Testing. In *Proceedings of the 2013 International Symposium on Software Testing and Analysis*, ISSTA 2013, pages 56–66. ACM, July 2013.