SPaCIoS

Secure Provision and Consumption in the Internet of Services

STREP Project number: 257876

Objective ICT-2009.1.4 c: Technology and Tools for Trustworthy ICT

01 Oct 2010 − 30 Sep 2013

www.spacios.eu

SPaCIoS

The Consortium

Academia

- Università di Verona (I)
- ETH Zurich (CH)
- Grenoble INP (F)
- KIT Karlsruhe (D)
- Università di Genoa (I)

Industry

- SAP Research (F)
- Siemens AG Munich (D)

Expertise

- Service-oriented architectures
- Security solutions
- Standardization and industry migration
- Automated security validation
- Formal methods and testing
- Security engineering

SPaCIoS

Services and their main stakeholders

- **Services provide business functionalities**

  - Business functionalities are typically the result of composing distributed services

  - Services include web-based applications and web services

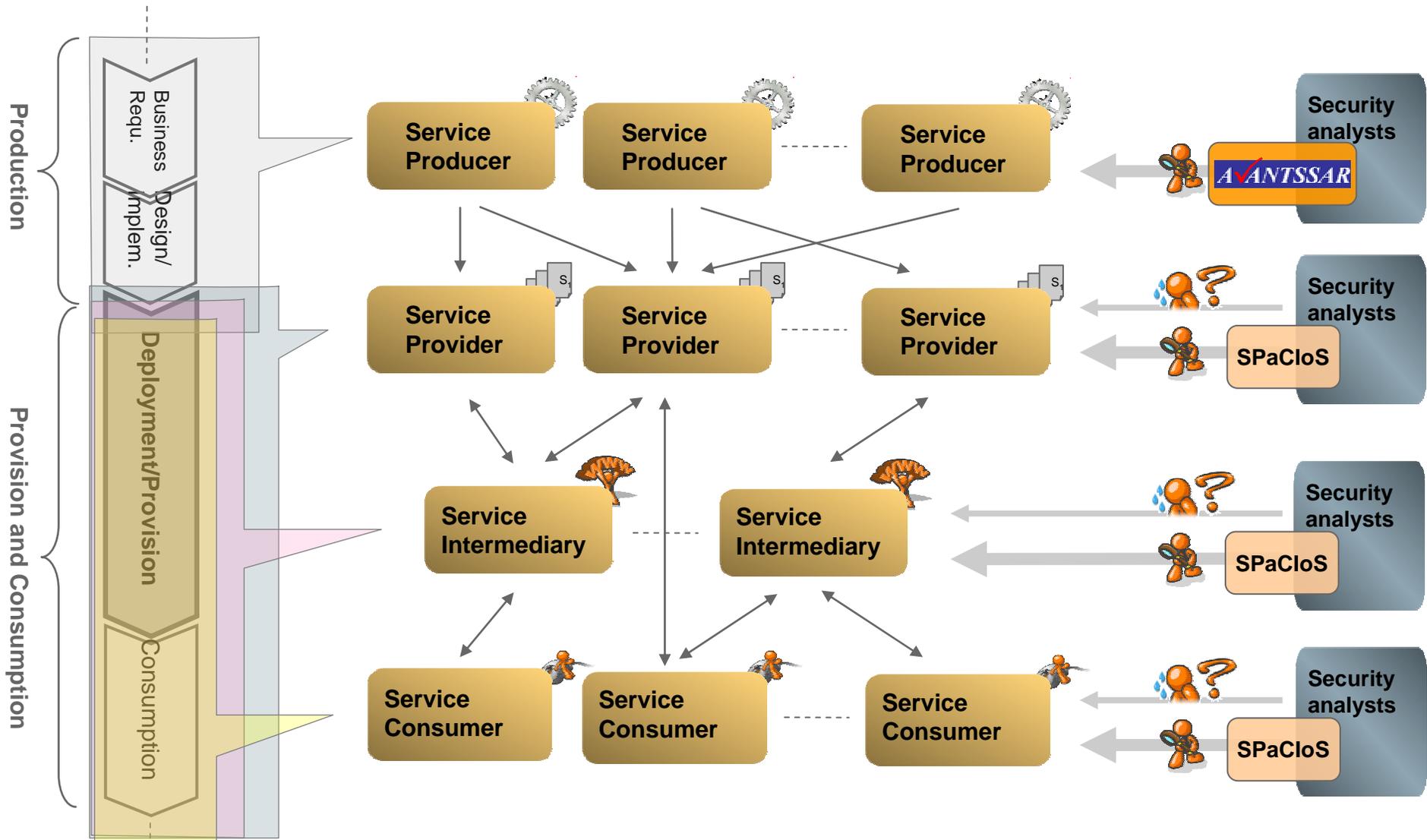 - Services do not imply any specific technology for implementing them

- **Four main service stakeholders (having their own security requirements)**

  - **Producers**: design and implement services

  - **Providers**: provide and deploy services

  - **Consumers**: consume services at runtime

  - **Intermediaries**: provide services to consumers by collecting services by providers

    - have specific trust relationships with consumers and providers

    - e.g., service brokers, service aggregators, etc

- **State of the art**

  - **Security analysts**: offer consultancy to stakeholders to analyze security requirements

  - **Existing tools**: not integrated, not based on a scientific approach, not at all automated, etc.

SPaCIoS

Scope of advancements wrt. state of the art

Production

Provision and Consumption

Business Requ.

Design/ Implem.

Deployment/Provision

Consumption

Service Producer — Service Producer — Service Producer

Service Provider — Service Provider — Service Provider

Service Intermediary — Service Intermediary

Service Consumer — Service Consumer — Service Consumer

Security analysts — AVANTSSAR

Security analysts — SPaCIoS

Security analysts — SPaCIoS

Security analysts — SPaCIoS

4

SPaCIoS

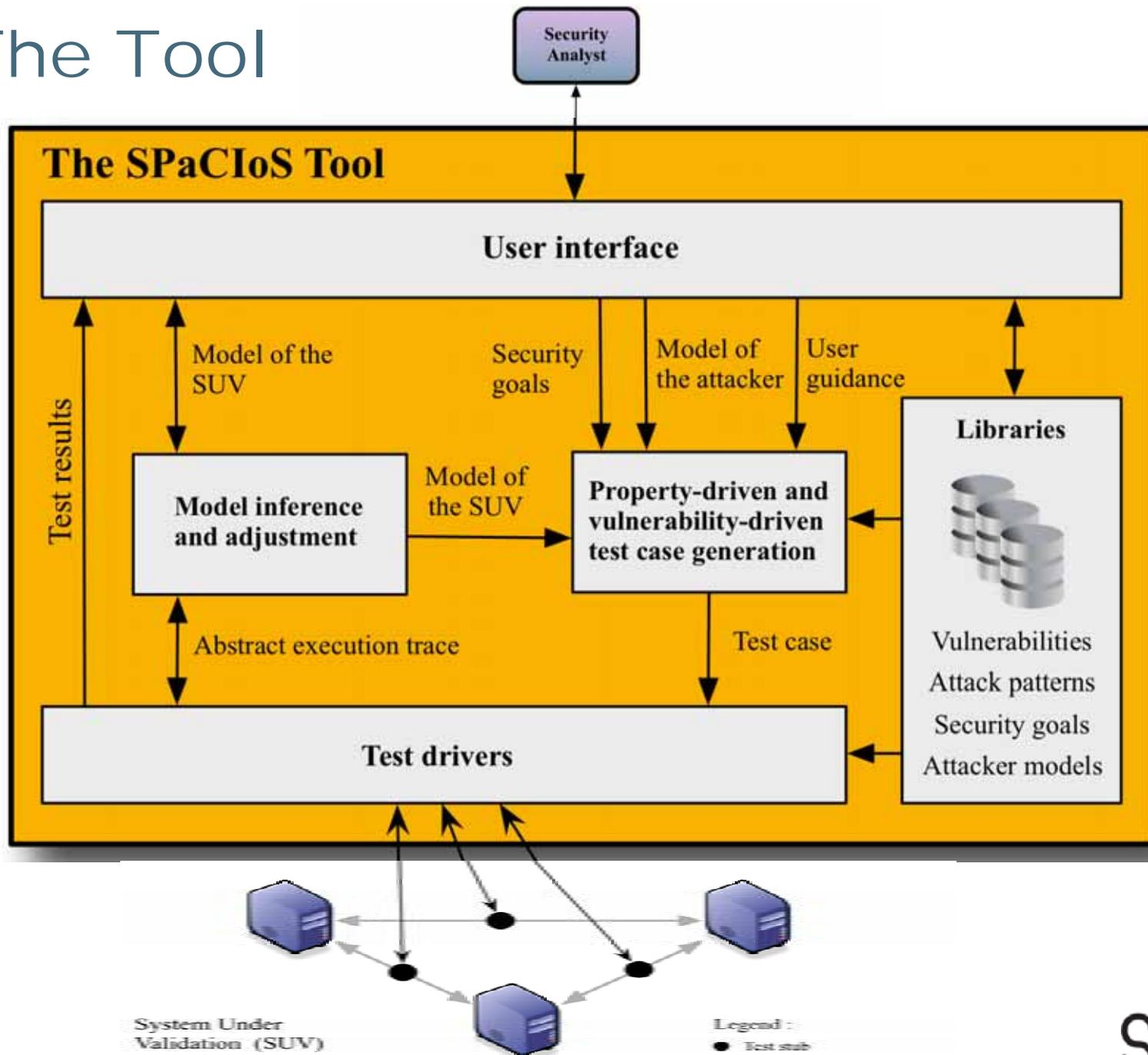# Project objectives and approach

Problems:

- To achieve the need guarantees to providers, intermediaries, and consumers of distributed services, rigorous security validation techniques must be applied.

- State-of-the-art security validation technologies fail to realise their full potential because they are typically used in isolation.

- Security validation in the Internet of Services (IoS) must be performed not only at production time, but also at deployment and consumption times.

Project objectives and approach:

- **Improve IoS security** by laying **technological foundations** of a new generation of security analysers for service deployment, provision and consumption.

- **Develop** the **SPaCIoS Tool** combining state-of-the-art technologies for penetration testing, model-based testing, model checking, and automatic learning.

- **Assess** the SPaCIoS Tool by running it against a set of security testing problem cases drawn from **industrial** and **open-source** IoS application **scenarios**.

- **Migrate** SPaCIoS technology to **industry** (SAP and Siemens business units), as well as to **standardisation** bodies and open-source communities.

SPaCIoS

The Tool

The SPaCIoS Tool diagram showing the Security Analyst connected to the User interface, which connects to Model inference and adjustment, Property-driven and vulnerability-driven test case generation, Libraries (Vulnerabilities, Attack patterns, Security goals, Attacker models), and Test drivers. Labels include: Model of the SUV, Security goals, Model of the attacker, User guidance, Test results, Model of the SUV, Abstract execution trace, Test case. Below: System Under Validation (SUV). Legend: Test stub.

Impact

Strategic impact: a novel technology (SPaCIoS Tool) for security analysts

- will strengthen the EU position in laying the fundamentals for a trustworthy IoS

- has the potentialities to generate outstanding impact on EU industry and standards

- will leverage on the traditionally European competence areas of formal methods, automated reasoning, and model-based security testing

Tight relation to, and possible collaboration with, other EU and international projects (including previous projects of the consortium members)

Plan for the use and dissemination of foreground:

- Early and continuous **dissemination**, through standard or dedicated/novel channels

- Meetings and workshops (*Expert Group*) covering broad range of target audience groups (system developers, business associations, standardisation bodies, journalists, citizen)

- An elaborated **exploitation plan** is provided, especially by industrial partners

- SPaCIoS has the potentials to generate remarkable impact at the **business environments** of its industrial partners (>30 PMs will be dedicated to actually execute this exploitation)

SPaCIoS

Backup

SPaCIoS Work Packages

WP2
Methodology, Models, and Security Properties

WP3
Validation Techniques

WP4
Validation Tools

WP5
Proof of Concept

WP6
Dissemination & Industry Migration

WP1

Project

Manage

-ment