Summary

- Project description
  - Project overview
  - ASSERT4SOA scope
  - Current vs. Improved SOA system
  - Overview of ASSERT4SOA activities
  - The Advisory Board
  - The first year of activities

- CC-relevant topics
  - ASSERT4SOA view of Certification Process
  - Possible use of pre-existing certification processes in the ASSERT4SOA context
  - Possible use of CC certification in the ASSERT4SOA context
Project Overview (1/2)

- Advanced Security Service cERTificate for Service Oriented Architecture (ASSERT4SOA)
  - Seventh Framework Programme
  - Area of Activity: Trustworthy ICT - ICT-2009.1.4
- Project web site
  - http://www.assert4soa.eu
- ASSERT4SOA Newsletter
  - Subscription is possible via the project web site
- Duration
  - 3 years (starting at October 2010)
Project Overview (2/2)

- 7 Partners
  - SAP AG (Germany)
  - Università degli Studi di Milano (Italy)
  - Universidad de Malaga (Spain)
  - Fraunhofer Gesellschaft zur Förderung der Angewandten Forschung e.V. (Germany)
  - Engineering Ingegneria Informatica (Italy)
  - City University of London (UK)
  - Fondazione Ugo Bordoni (Italy)

- 9 Work Packages (WPs)
  - To be introduced below
ASSERT4SOA scope

- ASSERT4SOA mainly aims at improving current SOA (Service Oriented Architecture) systems by making it possible for a service consumer to specify, for the service of interest, not only standard properties (e.g., functional ones), but also ICT security properties and corresponding assurance.

- A key role in this improvement is played by a digital certificate called ASSERT (Advanced Security Service cERTificate) which is specifically designed to:
  - Provide assurance about the security properties of a service
  - Be automatically processable (e.g., machine-readable, automatically comparable with other ASSERTs, ...)

FUB - 12th ICCC - September 27th, 2011
Current SOA system (1/2)

- A **service** is an autonomous unit of logic which is designed to accomplish a well-defined task (T. Erl, “Service-Oriented Architecture Concept, Technology, and Design”, Prentice-Hall ed., 2005)

- A **service description** includes (at least)
  - Name of the service
  - Location of the service
  - **Functional properties** of the service

- A service description could provide other information (e.g., **Security properties**)
Current SOA system (2/2)

- **Registration:** A service description is registered with a **Service Registry**, which provides **Service Discovery** based on standard criteria (e.g., functional properties)

- **Request:** A **Service Consumer** looking for a service forwards a specific **query** (covering standard service discovery criteria) to the service registry

- **Response:** The service registry responds with the list of links to the services that match the query

- **Interaction:** The service consumer interacts with a service in the list
Improved SOA system (ASSERT4SOA)

- **Registration**: ASSERT aware Service Discovery (see next slides) includes a service registry and is able to register and manage a service description that includes one or more ASSERTs for the service.

- **Request**: ASSERT aware service discovery is able to manage a query specifying extended service discovery criteria including:
  - The security properties requested for the service.
  - The respective assurance requested about such security properties.
Overview of ASSERT4SOA activities (1/4)

- The ASSERT4SOA activities focus on the definition of a specific part of the improved SOA system – the ASSERT4SOA Framework – and on the implementation and validation of a prototypical system.
- For this purpose, ASSERT4SOA is defining format and contents of the ASSERT (to be used to capture the results of a security certification process for a service).
- To provide an evaluation of the project results along the project duration, ASSERT4SOA is establishing and managing an appropriate Advisory Board.
Overview of ASSERT4SOA activities (2/4)

- The ASSERT4SOA Framework is the key component of the ASSERT aware service discovery and interacts with some external entities (which are also part of the ASSERT aware service discovery architecture)
  - Service Registry (which provides service discovery)
  - ASSERT Registry (which is the reference ASSERT repository)
  - ASSERT Issuers (which populate the ASSERT Registry)
Main ASSERT4SOA Framework functionalities

- Manages extended criteria in the request of the Service Consumer
- Forwards to the Service Registry a query including only standard criteria
- Retrieves from the ASSERT Registry the ASSERTs of the services indicated into the response of the Service Registry
- Compares ASSERTs of different services in order to provide the Service Consumer with a list of links to the services, ranked according to the extended criteria provided in the request
Overview of ASSERT4SOA activities (3/4)

- Format and contents of the ASSERTs will be defined by
  - WP1 ASSERT model and language
- Three different types of ASSERT, depending on the nature of the proofs used in the relevant process, will be respectively defined by
  - WP3 ASSERT-O: Ontology based certificate
    - An ASSERT-O can be based on pre-existing certificates (e.g., a CC one)
  - WP4 ASSERT-E: Evidence based certificate
    - An ASSERT-E is based on evidence produced by appropriate tests
  - WP5 ASSERT-M: Model based certificate
    - An ASSERT-M is based on formal proofs derived by appropriate models
Overview of ASSERT4SOA activities (4/4)

- Components, architecture, specification/validation of the ASSERT4SOA Framework will be respectively defined by
  - WP2 ASSERT aware Service Based Systems Design and Deployment
  - WP6 The ASSERT4SOA Framework
  - WP7 Requirements, specification and validation of ASSERT4SOA

- The Advisory Board establishment and management will be part of
  - WP8 Dissemination & Standardization

- The overall project will be managed by
  - WP9 Project Management
Structure of ASSERT4SOA
The Advisory Board

- The Advisory Board (AB), which involves people from the real world of software security certification—especially from CC community—and other stakeholders as well, will provide an evaluation of the project results along the project duration.
- Participation on voluntary basis.
- AB has the following duties:
  - Reviewing and assessing project contribution
  - Monitoring of market evolution
  - Acting as a dissemination channel
  - Ensuring alignment of project objectives and activities with certification ecosystem.
Advisory Board composition

- The Advisory Board is constituted by people from the following organizations
  - OCSI, Organismo per la Certificazione della Sicurezza Informatica (Italy)
  - DFKI, Deutsche Forschungszentrum für Künstliche Intelligenz (Germany)
  - Siemens (Germany)
  - CESG, Communications-Electronics Security Group (UK)
  - Real Casa de la Moneda (Spain)
  - SAP AG (Germany)
  - Florida Atlantic University (USA)
  - Fondazione Ugo Bordoni (Italy)
Advisory Board Scheduled Meetings

- The AB meetings are scheduled as follows:
  - 18 November 2011, Rome
    - Milestone M1 - Requirements and High Level Design Principles will constitute the main input to the meeting
  - (tentatively) July 2012
    - Milestone M2 - Feasibility Prototype and Advanced Concepts will be provided as input to the second AB meeting
  - Reports of the meetings and of AB activities will be produced and provided to the project
The first year of activities (1/2)

- The first year of activities has focused on
  - Collecting requirements, draft models and languages
  - Defining high level design of the architecture
- Most significant achievements approached
  - First specification of the ASSERT language (WP1)
  - Specification of query language and mechanisms for ASSERT aware service discovery (WP2)
  - Collection of requirements for an ontology supporting certificates interoperability (WP3)
  - Specification of the building blocks of the process issuing ASSERT-E (WP4)
The first year of activities (2/2)

(Continued)

- Specification of formal models and their composition to support ASSERT-M issue (WP5)
- Specification of the high-level architecture of the ASSERT4SOA Framework (WP6)
- Collection of requirements for the ASSERT4SOA Framework (WP7)
I) Security properties (or equivalent statements) to be certified (e.g., in CC, the Security Objectives for the TOE (and other portions of ST, if needed))

II) Product (or equivalent representation) to be certified (e.g., in CC, the TOE)

III) Additional specifications for the Security Properties, and/or the Product, and/or the Certificate, and/or other (e.g., in CC, the requested EAL)
IV) Proofs that the Security Properties hold for the Product (under the Additional Specifications provided as Extra Input) (e.g., in CC, the results of the Evaluation Activities)

V) Reports specifying the Evaluation Activities along with the extent to which the Security Properties hold for the Product (under the Additional Specifications) (e.g., in CC, the ETR)

VI) Material to support and/or specify Certificate interpretation (e.g., in CC, the ST)
Assessment here means everything needed to produce the data to be included in the ASSERT

- Note that the specification of the Assessment stage is out of the scope of ASSERT4SOA

- ASSERT Issue essentially consists of data formatting and signature (and can be largely automated)
Possible use of pre-existing certification processes in the ASSERT4SOA context

- Two possibilities
  - Derivation of an ASSERT-O from the standard certificate (leaving the relevant certification process unchanged)
  - Adaptation of a pre-existing certification process to produce an ASSERT-E or an ASSERT-M (in addition to the standard certificate)
I) **ASSERT Profile** for Certification Process X

- ASSERT profiles (to be defined by WP1) are specific tools for representing pre-existing certification processes

II) In this context, P is a service

- ASSERT4SOA aims to support existing certification bodies in the assessment of services
ASSERT-O derived from pre-existing certificates (2/2)

- SP, P, EI, and X-Profile could be not available for the Interpretation stage (if X-Profile is missing, the specification of Certification Process X is required)
- Note that SP, P and EI for the Interpretation stage could be not coincident with those for the Certification Process X (e.g., only a subset of the original SP or P could be considered)
Certification Process Adaptation

- Two options for using a pre-existing certification process in the Assessment stage
  - Adapt only the Certificate Issue specifications
    - The Evaluation stage is not modified (desirable, but expected to be unfeasible)
  - Adapt also the Evaluation specifications
    - Probably, more flexible (or only possible) approach
Possible use of CC certification in the ASSERT4SOA context

- Possible contact points between ASSERT4SOA and CC certification
  - Derivation of an ASSERT-O from a pre-existing CC certificate
  - Adaptability of a CC certification process to produce an ASSERT-E
Some general Interpretation issues arise from this example

- CC Certificate and ST are not machine-readable (they are not forced to use a formal language, CC Certificates do not have a uniquely-defined structure...)

- CC Certificate could be not sufficient to generate ASSERT-O data, because the standard does not require to include the security properties for the TOE (e.g., ST is needed for this purpose)
How the CC community could help in dealing with the identified Interpretation issues
- Promote the use of a defined and shared structure for the CC certificate
- Promote the use of a semi-formal/formal language also for security objectives (define a catalogue)

How ASSERT4SOA could help the CC community in enhancing interpretability of CC certificates
- ASSERT profile for CC
Example of CC derived ASSERT-O (work in progress)

```
<Property>
  <ID>ao:AuditREAL3.CC.org</ID>
  <Description>The TOE has the ability to audit user actions and store the records in an audit trail that is protected from unauthorized access. The administrator has the ability to select which events get audited</Description>
  <FormalSpecification>
    <TypeOfSpecification> Link </TypeOfSpecification>
    <PropertySpecification> ..... </PropertySpecification>
  </FormalSpecification>
</Property>

<Property>
  <ID>ao:UserDataProtection@core</ID>
  <Description>The TOE provides a discretionary access control mechanism to protect user objects such as files, directories, and message queues. Resources are cleared of previous information before a user allocates them.</Description>
  <FormalSpecification>
    <TypeOfSpecification> Link </TypeOfSpecification>
    <PropertySpecification> ..... </PropertySpecification>
  </FormalSpecification>
</Property>
```

The ASSERT Issuer shall build the formal specification reading the whole CR and ST.

The descriptions are in natural language, so it’s difficult to compare properties of different TOEs.
ASSERT-E: Introduction

- ASSERT-E provides evidence-based proofs that a test carried out on the service has given a result
- ASSERT-E Issue (work in progress) is based on
  - A model for the specification of the security properties
  - A model for the specification of the test cases related to the security properties
**ASSERT-E: Model for security property specification (1/2)**

- **Abstract security properties**: Generic security requirements for the service under evaluation (e.g., Authenticity, Confidentiality, Integrity)
- **Property instances (to be certified)**: Abstract properties enriched with a set of attributes
  - Domain of each attribute has a partial/total order relationship
  - Example: Password-based authenticity

![Diagram showing the relationship between abstract security properties and property instances](image-url)
**Intra-property relationship**: Relationship between property instances that refer to the same abstract property, defined based on class attributes (e.g., Authenticity with PWD and token ⪰ Authenticity with PWD only)

**Inter-property relationship**: Equivalence or order relationship between property instances that refer to different abstract properties, defined based on the expert knowledge (e.g., Non-repudiation ⪰ Integrity)
**ASSERT-E: Model for test case specification**

- Each security property is associated with one or more **test classes** (e.g., **functional** and **penetration**, which can be respectively mapped to the ATE_IND and the AVA_VAN activities in CC)
- Each test class contains a set of **test types**
- Test types are organized in **hierarchies**

![Diagram of test classes and test types]
Adaptability of a CC certification process to produce an ASSERT-E (1/2)

- In order to issue also an ASSERT-E for a service under CC certification, the CC evaluation process could be adapted by including
  - A formal specification for security properties of the TOE, similar to the model presented before
  - A formal specification for tests performed on the security properties of the TOE
Adaptability of a CC certification process to produce an ASSERT-E (2/2)

- The formal specification for security properties can be
  - Provided by the sponsor
  - Elaborated by the evaluator (from the ST)
- The formal specification for test cases
  - Can be provided by the sponsor wrt the functional tests
  - Should be elaborated by the evaluator wrt the penetration tests

FUB - 12th ICCC - September 27th, 2011
Thank you

morazi@fub.it

vbagini@fub.it (contact author)