Answers to Open Issues from Reviewer

pSHIELD Review Meeting

Kjeller/Oslo, *29-30th September 2011*

ARTEMIS Call 2009 – SP6100204

SESM A Finmeccanica Company · Thyia Technologies · Sapienza Università di Roma · Hellenic Aerospace Industry · EuroTecH The complete embedded PC solution · MOVATION · ELSAG DATAMAT A Finmeccanica Company
Critical Software · DIBE · SELEX Communications A Finmeccanica Company · I.S.I. Industrial Systems Institute · MONDRAGON UNIBERTSITATEA · ESI European Software Institute tecnalia · AnsaldoSTS A Finmeccanica Company · ISD S.A. Integrated Systems Development · CWI · Tecnologie nelle Reti e nei Sistemi T.R.S. SpA

Open Issues Overview

- Following mid-term review meeting held in Brussels in march several open issues were raised by Reviewer
- Answers to open issues have been provided by pSHIELD Partners and uploaded on wiki collaboration tool
- A brief presentation related to open issues answers will follow describing how the answers have been provided and then focusing on answers' content

#1 Anticipated Deliverables' Availability

A special page at pSHIELD Wiki was created containing a list of all deliverables with links to their electronic versions:

http://pshield.unik.no/wiki/Deliverables_for_JU

Most of deliverables have been uploaded on 16th of September and the last ones by 20th of September

#2 Paper & Electronic Presentations Copies

- No answer has been provided in the answer document since the issue is related to a specific action and the issue is considered addressed when the action is performed

- The paper copies of all presentations have indeed been provided at the start of the review meeting and their electronic copies are available on the wiki

#3 Presentations Tips

- Also in this case no answer has been provided in the answer document since the same reasons as previous open issue apply

- The presentations' content has been revised in order to meet reviewer's tips

#4 Additional Documents Due in Mid April

All requested documents were provided to JU in due time. All the documents are available in electronic form in project repository at bscw server:

http://bscw.juartemis-pshield.eu/bscw/bscw.cgi/12529

Folder: Mid-term review additional deliverables

Sub-folders: Point 1 to Point 6

#5 Masters and PhD thesis list

A list of PhD thesis initiated or executed within pSHIELD has been provided and can be found in D7.1.2 Dissemination Report too

#6 Key Achievement and Breakthrough

A list of key achievements of pSHIELD project has been provided comprising:

- Identification of pSHIELD semantic technologies (to model SPD issues)
- Semantic models to enable the pSHIELD seamless approach definition of main services at middleware layer
- Prototypes of ontologies
- Prototypes of semantic patterns of SPD composition
- Experimental semantic engine for SPD composition
- Analysis of the OSGI Knoplerfish platform as technological demonstrator for pSHIELD Middleware
- Service Oriented technology selection to address the seamless approach and interoperability requirements

#7 Website upgrade

The project on-line collaborative tools are composed of three elements:

- Semantic Wiki (for Partners' technical discussions, agendas, minutes, meeting, phone conferences, etc.)
- **Website (to communicate project achievements to wide audience)**
- Secure Repository (to manage important documents)

Efforts have been made to keep Website updated and informative

#8 Publications lists

In the frame of project dissemination tasks on pSHIELD Wiki is available a page listing:

- Targeted Industrial Dissemination
- Workshops and Exhibitions
- Industrial publications
- Scientific dissemination

The dissemination page is continuously updated. Electronic copies of most important materials are also available at the Wiki page

#9 Answers to Open Issues

A file has been created and is available on Wiki containing explicit responses to each open issues

#10 Glossary Document

A dedicated Wiki page was created to answer that question:

http://pshield.unik.no/wiki/Terms_and_Definitions

#11 Composition Topology Discrepancy (1/2)

There is no discrepancy between M0.1 and M0.2 documents since they address two different concepts, respectively:

- **Composition topology** (the admissible ways to compose SPD components, each one providing a specific SPD functionality with a defined SPD value, for the purpose of obtaining different configurations to choose from in order to guarantee a target SPD value)
- **Composition algebra** (a way to calculate the SPD value of a system once defined the SPD value of each component)

#11 Composition Topology Discrepancy (2/2)

Concerning **composition topology** the pSHIELD envisages a n:m topology. Each SPD component can be composed simultaneously with one or more SPD components. The composability rules are specified both within the formal description of each SPD functionality and pSHIELD architectural choices. These rules are managed by the Overlay layer.

Relating to **composition algebra** described in M0.2 it comes from the medieval castle theory. This algebra is constructed considering repeatedly a pair of SPD components and applying them one of the defined operators depending on the fact that the two considered components provide functionalities working in parallel, concentric or concurrent way. Only the graphical representation of the composition algebra as a tree having the SPD components as leaves is a hierarchical one but it has nothing to deal with composition topology

#12 Composition Algebra Completeness

- The composition algebra is not complete, but enough for a pilot project and to address Technical Annex, whose objective is to “demonstrate composability”.
- The selected algebra demonstrates that SPD functionalities can be composed and the result of composition can be correctly quantified according to specific metrics.
- The operators are not so few and simple as it can seem at first glance. Actually the operators are: MIN, OR, ORn, MEAN, POWER MEAN and they are able to model several situations such as redundancy of SPD functionalities, honeypot solutions, aimed at distracting attackers from attacking more valuable items, and other cases where different degrees of knowledge of the defenders or of the attackers are considered

#13 pSHIELD SPD catalog and real world examples

- An outlook of a full set (not complete and not consistent) of SPD properties is shown in D2.2.1 Annex A
- An example of a typical topological configuration is present in D2.2.1 in section 8.1.4
- More detailed examples will be present in D2.2.2 final version

#14 M0.1 and M0.2 Acceptance by All Partners

- New deliverables M0.1 and M0.2 are listed with full names in M0.3 Signed Endorsement, and all project partners accepted and signed M0.3
- The works on M0.1 and M0.2 were conducted by all partners, and draft versions exchanged and discussed by means of Wiki, emails and phone conferences
- The list of members in M0.1 title page represents only the core team maintaining the document on behalf of all partners

#15 Functional Architecture not Formally Elaborated

The architecture should be generic enough to fit each operating context, and this is the motivation of figure 3.8. Some adjustment will be done and inserted in the architecture document

*Note: The TA uses "formal concepts". Our goal was to use formal descriptions to some extent. In this **pilot** we focus on a bottom-up approach with formal descriptions of individual devices.*

*A fully formal model for **Shield** would require a project on it's own; we intend to increase formal descriptions for the development of Shield.*

#16 Control Algorithm not Sufficiently Elaborated

- The control algorithms, together with the common criteria approach and the policy based management, are a set of rules and mechanism to “control” the evolution of the system towards a desired one
- Since the pilot project is not supposed to address the dynamic monitoring and reaction, these control algorithms are not implemented or designed, but simply introduced towards simulations as D5.2 prototype
- The selected control algorithms are based on optimization (like, for example, model predictive control)

#17 SPD Metrics and How to Measure Them (1/2)

- Deliverables D2.2.1 and D2.2.2 contain a detailed description of the SPD metrics proposed and how they will be measured
- Particularly the SPD metric definition is based on fault prevention, tolerance and removal
- Each identified SPD function will be characterized by a value that will indicate how much is valid the implementation of that particular functionality to face faults of the pSHIELD system
- The SPD level that will be attributed to the whole pSHIELD system matches with the product of the pSHIELD SPD functional components value and the pSHIELD SPD life cycle support components value

#17 SPD Metrics and How to Measure Them (2/2)

- pSHIELD SPD functional components value will be calculated through vulnerability assessment and penetration tests according to Common Criteria approach

- pSHIELD SPD life cycle support components value will be calculated through an analysis of these support components performed according to Common Criteria rules

#18 Cryptographic technologies

- After choosing the most suitable cryptographic paradigms, two different cryptographic algorithms will be tested in different platforms similar to micro and/or power nodes

- Deliverable D3.4 will contain detailed information about these tests as well as a technical description about the most innovative objectives to be achieved in pSHIELD project: the new cryptographic key exchange algorithm (called “Controlled Randomness”)

#19 Ontology Concepts Detailed Description

- D5.1 shall cover the ontological modeling of SPD, and show in what way the ontology provides “semantic glue” in order to support interoperability and composition processes
- The ontological model (i.e. the prototype) has been developed and is available in D5.1, as well as some consideration about its implementation (that may be put also in D5.3)
- In particular the mechanism to store and process ontology is implemented in a reduced scope in the OSGI framework (Java primitives)
- This problem will be addressed in a more structured way in the nSHIELD project

#20 SPD Core Services and SPD Functionalities

- **SPD core services** and **SPD functionalities** are different concepts
- The **SPD core services** regard pSHIELD middleware (composability, orchestration and discovery) and are described in D5.2
- **SPD functionality** is a software, hardware or firmware component of the pSHIELD that must be relied upon for the correct enforcement of the pSHIELD Security, Privacy and Dependability policy
- All the necessary **core SPD services** will be defined at node, network and middleware layer and relevant information about these services can be found in deliverables D5.2 and D3.4

#21 Run Time Monitoring

- The runtime monitoring is a nSHIELD concept, while the outcome of pSHIELD is to indicate whether the configuration satisfies the SPD desired levels or not and even to switch from one configuration to another equivalent

- In case of no satisfaction, the configuration is simply not actuated

- However, from the analysis of the architecture of pSHIELD Middleware, the composability orchestrator is replicated in more components in order to improve dependability

#22 Hybrid Automata Concept

- In D5.4 a more comprehensive state of the art and academic dissertation is included to justify the choice related to hybrid automata
- Surely the hybrid automata theory introduces some implementation issue that can be solved by adopting a scalable approach (from policy based management, to semantic inference)
- Some considerations are already present in D5.2

#23 How CC are applied in pSHIELD?

- In D2.2.1 (Chapter 5) The Common Criteria (CC) standard application into the pSHIELD methodology/framework is described in detail
- Since pSHIELD framework is not oriented to a specific application, we have not considered any specific safety and security standard
- However in the CC vulnerability assessment, which leads us to define the SPD value, we can consider any specific standard in order to take into account specific threats or specific application scenario concerns