SHIELD
PILOT

The pSHIELD experience: Achievements, Breakthroughs and Challenges

pSHIELD Final Review Meeting

Bruxelles, *14th February 2012*

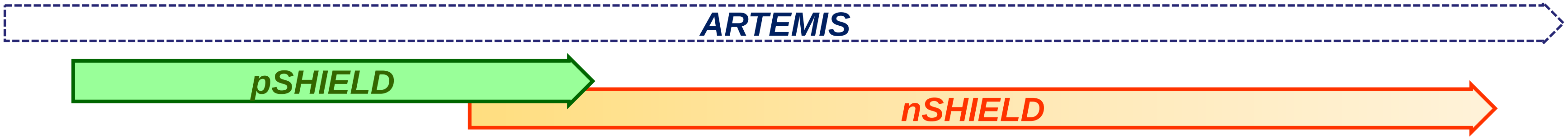
Andrea Fiaschetti

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 · AC · Tecnologie nelle Reti e nei Sistemi T.R.S. SpA

Introduction

After 19 months of activities, the pilot phase of the SHIELD roadmap has been completed and it is time to check what has been achieved, what is really a breakthrough and what has raised new promising challenges.



The pSHIELD project was basically supposed to be a proof of concept.

But of what concepts? The Technical Annex mentions the following ones:

1) Demonstrate composability
2) Develop new technologies
3) Assure Modularity and expandability
4) Design Architectural Framework
5) Define Metrics
6) Demonstrate into an Application scenario

pSHIELD Assets

We have produced **tangible assets** to sustain our proof of concepts:

- 28 official deliverables (plus 6+2 additional deliverables)
- a dozen of prototypes
- several papers, Ph.D. and master thesis
- participation to dissemination events

But the pSHIELD biggest outcomes, that enrich the value of the paperwork, HW and SW produced so far, are the “**ideas**” behind those outputs, and the “**perspectives**” that they open. They will be our major achievements.

As usual, the major achievements are grouped in three areas:

- Consortium and management activities
- Scientific and Technological Achievements
- Impact, visibility and business opportunities

Consortium and management activities – WP1

Major Achievements:

- Clear definition (and agreement) of roles
- Capitalization of knowledge
- Improved information availability and common awareness on project outcomes
- Liaison with the second phase thanks to the involvement of nSHIELD coordinator
- Continuity assured by the presence of key personnel

Breakthroughs

- At the beginning of pSHIELD we were a consortium working on a project. Now we are a team working for a common goal: make pSHIELD a reality.

Measurable outcomes:

- Consolidation and intensive use of Wiki
- Delivery of all documents
- Project completion in time

New Challenges

- Perform a seamless handover towards nSHIELD

Technological Achievements – WP2

Major Achievements:

- Identification and formalization of a coherent SPD Metric
- Formalization of two methodologies to compose SPD Metrics

Breakthroughs

- Compliance with the existing standard Common Criteria (ISO 15408)
- Consistently measured, without subjective criteria
- SPD level not expressed using at least one unit of measurement (defects, hours, …)
- Expressed as a cardinal number
- Context specific, relevant enough to make decisions

Measurable Outcomes:

- D2.2.1-2 pSHIELD SPD Metrics
- Implementation of one of these methodologies into WP5 prototypes with the semantically-enabled metrics composition

New Challenges

- Extend and enrich the approach to capture the complexity of composition

Technological Achievements – WP3 (1/2)

Achievements:

- Development of extensive set of Node requirements that exactly address the goals of Technical Annex.

- Design of *generic conceptual model* of a pSHIELD node for all node types, which can be implemented in different architectures, providing different functionalities, different SPD compliance levels and different services, depending on the type of node and application field. Three node types represent very different devices but they share the same conceptual model, enabling a seamless composability.

- Power Node PCB Layout design completed

- Study on cryptographic solution for all kinds of nodes with limited resources

- Design and implementation of a protection circuit for a power supply (dependable power supply)

Breakthrougs:

- Node secure and dependable by construction

- Development and implementation of application: Dynamic Reconfigurable Node

- pSHIELD node installation was the first on M2M platform

Technological Achievements – WP3 (2/2)

Measurable Outcomes:

- D3.1-2-3-4

- pSHIELD SPD FPGA Power Node prototype

- Protection board prototype

- Integration with Telenor Shepherd® Platform

- Connectivity with Shepherd® Platform
 Prototype of cryptographic algorithms into a micro node (TelosBmote)

Challenges

- Composability with pSHIELD network

- Cover the chain to certify the Softcore (never certified)

Technological Achievements – WP4 (1/2)

Achievements:

- Development of a real Cognitive Radio Node software that is able to automatically detect the presence of a threat and adjust internal radio transmission parameters accordingly

- Realization and adaptation of HW and SW of multicore platform for the cognitive algorithm validation on embedded system

- Implementation of a Cognitive Radio Node software simulator

- Identification of spectrum sensing features for Cognitive Radio analysis

- Adaptation of sensing part of the Cognitive Radio simulator for pSHIELD

- Study of the requirements for lightweight link-layer secure communication in wireless sensor network scenarios and the design and development of proper schemes focusing on confidentiality. More specifically, intrusion detection systems (IDS) have been studied.

- Study of the resource footprint (energy consumption among them) and its impact on performance on some commercially available devices.

- Studies on the setup of a general framework for secure communications within heterogeneous networks comprising resource-limited devices

Technological Achievements – WP4 (2/2)

Breakthroughs:

- Miniaturization of Cognitive Radio Technologies

Measurable Outcomes:

- D4.1-2

- Network prototypes:
  - Innovative approaches for SPD driven transmissions and Trusted and dependable connectivity
  - Spectrum Sensing for SPD driven transmissions and Trusted and dependable connectivity
  - Physical layer Techniques enabling SPD driven transmissions and Trusted and dependable connectivity

Challenges:

- Implement Cognitive Functionalities: cognitive resource management, spectrum-aware routing, …

Technological Achievements – WP5 (1/3)

Achievements:

- Semantic model compliant with defined metrics

Breakthroughs:

- Definition and implementation of an original ontological model of ESs, including the semantic characterization of the system and inferential engine features (based on specific metrics) to face the SPD composability problem

Measurable Outcome:

- D5.1-3
- A prototype owl file with the pSHIELD Ontology has been obtained
- A prototype of reasoner has been integrated into the pSHIELD Middleware emulator

Challenges:

- Enrich and refine the semantic model to reinforce the composability mechanism

Technological Achievements – WP5 (2/3)

Achievements:

- Design and implementation of a reduced but significant “working” example of the pSHIELD Middleware and Overlay. This Middleware is able to discover and compose SPD functionalities to achieve the desired SPD level.

- Technological Assessment of the Policy Based Management for Security applications and preliminary feasibility analysis with respect to pSHIELD

- Formulation of an innovative model to represent (composable) Embedded Systems based on the theory of Hybrid Automata. Thanks to this formulation it has possible to apply some closed-loop control algorithms (like MPC) to optimize the SPD composability in a context-aware way.

Breakthroughs:

- Harmonization of control algorithms, Policy Based Management and Common Criteria approaches in the Security Agent architecture

Measurable Outcomes:

- D5.2-4

-OSGI prototype of pSHIELD middleware performing composability tasks in collaboration with CS nodes

Technological Achievements – WP5 (2/3)

Challenges:

- Replicate this environment on a real world middleware
- Improve the overlay behaviour by enabling interaction between Security Agents
- Enrichment of control algorithms (i.e. DES Theory)

Technological Achievements – WP6

Achievements:

- Definition of the use case environment in the form of freight trains transporting hazardous material

- Demonstration of the usability and transmission of data produced by sensors, in the service of specific use case scenarios as critical infrastructure protection

- Exploration of the platform's synthetic capability and composability, through possible synergies and fusion/cooperation of components

Breakthroughs:

- Identification of several prototypal demonstrators to demonstrate the interoperation among different (composed) technologies and the possibility of realizing SPD functionalities

Measurable Outcomes:

- D6.1-2-3-4

- Prototypal Demonstrators

Challenges:

- nSHIELD new scenarios and technologies

Prototypal Demonstrators: SPD Functionalities

FPGA Power node prototype (SPD)
SPD metrics, Self-recovery from hardware transient faults (through fault-injection), Auto-reconfiguration, Data encryption, Provision of security and privacy services, Hardware data encryption/decryption

Cognitive Radio prototype (SPD)
Threats tolerant transmission

Middleware prototype for composability (SPD)

SPD Audit, Cryptographic Support, Identification and Authentication, Protection of the SPD functionalities, Security Management

Heterogeneous Platform prototype (SPD)
Auto start up on power failure, Auto reconfigurable on software failure, Auto synchronization on software failure, End-to-end secure communication, Mal-user detection, Access control for accessing sensor data

Rail car monitoring system (SPD)
Intrusion awareness, fault-tolerance, data redundancy and diversity

Impact, visibility and business opportunity – WP7

Achievements:

- Targeted dissemination at top level, including telecom actors (Telenor), industrial actors (ABB) and security research institutes (Norwegian Defense Research Establishment)

- Real world interworking of sensors on the measurement locomotive of the Norwegian Rail Authorities and Telenor Objects

- pSHIELD implementation in place in an electrical motorcycle at the showroom of Telenor, the Innovation Fair at Fornebu

- Foundation of IoT/Future Internet *Value Network* for Industrial Ecosystem

Breakthroughs

- Awareness of the IoT Ecosystem for semantic-based security

New Challenges

- Scalability: Transformation from SPD sensor to SPD application

Measurable Outcome:

- Dissemination and Exploitation reports

- Field trials

Conclusions

In our reduced but still significant context we have learned that:

- It is possible to define the characteristics of a pSHIELD component and of the pSHIEL system (*Design Architectural Framework*)

- It is possible to quantify security, privacy and dependability (*Define metrics*)

- It is possible to improve SPD technologies (*Develop new technologies*)

- It is possible to compose SPD technologies according to the selected metric (*Demonstrate composability*)

- The composability mechanism is independent to the number and type of underlying technologies (*Assure Modularity and expandability*)

- It is possible to provide enriched services and application to relevant application scenarios with SPD requirements (*Demonstrate into an Application scenario*)

…so it seems worthwhile to continue this “research adventure” by leveraging the lessons learned up to now towards more challenging results.