SERENITY

System Engineering
for Security & Dependability

Dynamic Security in Ambient Intelligence Scenarios

Antonio Maña – Research Director

Introduction
What is SERENITY about?

Security in Ambient Intelligence Scenarios

- Defined by the EC Information Society Technologies Advisory Group (ISTAG), ***Ambient Intelligence*** (AmI for short) emphasises on greater user-friendliness, more efficient services support, user-empowerment, and support for human interactions.
- In this vision, people will be surrounded by intelligent and intuitive interfaces embedded in everyday objects around them and an environment recognising and responding to the presence of individuals in an invisible way by year 2010.
- **Ambient Intelligence** builds on three recent key technologies:
  - **Ubiquitous Computing** means integration of microprocessors into everyday objects like furniture, clothing, white goods, toys, even paint.
  - **Ubiquitous Communication** enables these objects to communicate with each other and the user by means of ad-hoc and wireless networking.
  - **Intelligent User Interfaces** enable the inhabitants of the AmI environments to control and interact with these environments in a natural (voice, gestures) and personalised way (preferences, context).
- The ISTAG vision is that AmI applications will be influenced by the computational, physical and behavioural contexts that surround the user (for instance, because of resource availability and security or privacy requirements).

Introduction
What is the problem?

- The concepts of ***system*** and ***application*** as we know them nowadays will disappear,
  - evolving from static architectures with well-defined pieces of hardware, software, communication links, limits and owners,
  - to open architectures that will be sensitive, adaptive, context-aware and responsive to users' needs and habits that we will refer as ***AmI ecosystems***.
- These ecosystems will offer highly distributed dynamic services in environments that will be heterogeneous, large scale and nomadic, where computing nodes will be omnipresent and communications infrastructures will be dynamically assembled.
- The provision of security and dependability for these ecosystems will be increasingly difficult to achieve with existing security solutions, engineering approaches and tools because of the combination of
  - heterogeneity,
  - dynamism,
  - along with the growing demands for dependability and security,

Challenge 1:
Dealing with dynamism

- In the new AmI scenarios, not only systems as a whole but also individual applications running in or supported by those systems will have to ***adapt to dynamic changes to hardware and software, and even firmware configurations, to unpredicted and unpredictable appearance and disappearance of devices and software components***. In other words applications must be able to adapt dynamically to new execution environments. Pre-defined trust relationships between components, applications and their system environments can no longer be taken for granted.
- The increased complexity and unbounded nature of AmI applications make it impossible, even for the most experienced and knowledgeable S&D engineers, to foresee all possible situations and interactions which may arise in AmI environments and therefore create suitable solutions to address the users' security and dependability requirements.
- S&D engineers will be faced with pieces of software, communication infrastructures and hardware devices not under their control. Thus, approaches based on the application-level security will not be sufficient.

Challenge 2:
Dealing with heterogeneity

- AmI environments will contain a large number of ***heterogeneous computing and communication infrastructures and devices*** that will provide new functionalities, enhance user productivity, and ease everyday tasks.
- These devices will hold a variety of data with different security and privacy requirements.
- This information will be used in different ways in different applications and computing contexts and, therefore, different policies (possibly contradicting) will be applied.
- In such settings, securing the device or the information alone or even each individual application is not sufficient, and context information should be integrated in order to be able to choose appropriate security mechanism on-the-fly.

Challenge 3:
Need for supervision

- Because of their complexity, and because elements will be under the control of different owners, security mechanisms will ***need to be supervised*** (monitored) in order to identify potential threats and attacks and decide on recovery actions, when possible.
- Some existing approaches can provide suitable solutions to support the dynamic evolution of security policies for specific security mechanisms - e.g. SAC model for access control- at particular system operation layers (application, networking).
- However, these approaches cannot be extended to support the dynamic evolution of general security mechanisms (as opposed to security policies for a single mechanism).
- Furthermore, their results are extremely complicated to integrate, monitor and dynamically evolve as would be required by AmI ecosystems.
- For the very same reasons, S&D approaches for AmI ecosystems cannot hope to synthesize new S&D mechanisms or new combinations of these mechanisms fully automatically and dynamically.

Challenge 4: Dynamic application of security expertise

- We can summarize the individual challenges that we have devised so far into a simpler and yet tougher grand challenge:
- ***The provision of S&D in AmI ecosystems requires the dynamic application of the expertise of security engineers*** in order to dynamically react to unpredictable and ever-changing contexts.
- The intuitive solution would be to create an "intelligent" system able to analyze the requirements and the context in order to synthesize new solutions.
- Unfortunately, given the state of the art in both security engineering and intelligent systems, this approach is not a promising one in the foreseeable future.
- To meet this challenge in our time we need to look more closely to what technology is available for S&D mechanisms in AmI ecosystems.

Then, what is the key for this problem?

- Providing security in heterogeneous and dynamic computing scenarios requires the ***dynamic application of the expertise of security engineers***.
- SERENITY aims at capturing this expertise and making it available in the above-mentioned scenarios
- ***S&D Patterns*** and ***Integration Schemes*** are the means, complemented by ***Runtime Monitoring*** mechanisms and tools

SERENITY Mission Summary

Develop ***mechanisms and tools*** for the automated provision of ***security and dependability*** in ***AmI ecosystems***

by ***capturing the security and dependability expertise*** in the enhanced concept of ***Security and Dependability Patterns*** and ***Integration Schemes***

with an approach cutting through and integrating three levels of abstraction:
Business Organization level
Workflow and Services level
Network and Devices level

in the challenging context of the AmI Ecosystems.

Technical Challenges & proposed apAroach (I)

C Characterization, verification and validation of reusable security solutions

A Enhanced notion of Security and Dependability (S&D) Patterns and Integration Schemes

- Basic Building Blocks: **SERENITY's S&D Patterns** are precise specifications of simple (reusable) security solutions featuring an operational functional description of the solution; and a semantic-based description of
  - i. the security requirements addressed;
  - ii. descriptions of any preconditions or assumptions that govern the deployment of the pattern;
  - iii. description on how to monitor the behaviour; and
  - iv. trust mechanisms.
- Integration: **SERENITY's Integration Schemes** specify ways for systematically combining S&D patterns and integrating them in systems composed of statically or dynamically collaborating elements that operate in mobile and highly dynamic ICT infrastructures.

Technical Challenges & proposed Approach (II)

C Automated processing of security requirements

A SERENITY Framework

- Definition of a library of S&D patterns and Integration Schemes including formally characterized behaviour and semantics
- Tools for automated classification, selection and composition of solutions
- Support for the run-time pro-active and reactive identification of potential threats and attacks of implemented security solutions

SERENITY’s Results:

- **Security & Dependability Patterns** and **Integration Schemes**
  - A **model** and **associated procedures**
  - **Tools** to create and manage S&D patterns and integration schemes
    - **analyse S&D solutions at different abstraction levels**
    - **specify and manage S&D patterns and IS**
    - **provide trust in the solutions and their specifications**
    - **support evolution of S&D patterns and IS**
  - A **collection** of S&D patterns and integration schemes
    - Specific S&D mechanisms
    - Associated descriptions

- SERENITY’s **Integrated Framework** consisting of S&D patterns, integration schemes, and tools to manage, apply, and monitor them
  - **Tools** to use S&D patterns and integration schemes in AmI ecosystems
    - **integration of S&D patterns and IS in AmI ecosystems**
    - **monitoring of ecosystems based on S&D patterns and IS**
  - **Framework instantiations**
    - application of the SERENITY framework to a particular S&D development problem