Network of Excellence

Deliverable D4.1

Abstract

The deliverable presents the integration strategies that we are going to follow for each of the different communities and stakeholders interested in the area of secure service engineering.

This deliverable also shows a brief summary of the first version of the roadmap on secure service engineering that is aimed to build the future steps for the research community in the area.

Keyword list

Integrated agenda, research roadmap, integration tools
## Document History

<table>
<thead>
<tr>
<th>Version</th>
<th>Type of change</th>
<th>Author(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>V0.1</td>
<td>Initial ToC and contents for sections</td>
<td>Francisco Moyano, Carmen Fernández</td>
</tr>
<tr>
<td>V0.2</td>
<td>Sections 4, 5.1, 5.3, 6.4 and 7</td>
<td>Carmen Fernández, Francisco Moyano</td>
</tr>
<tr>
<td></td>
<td>Section 5.2</td>
<td>Gerardo Fernandez, Isabel Vinagre</td>
</tr>
<tr>
<td>V0.3</td>
<td>Updates of section 5.2</td>
<td>Isabel Vinagre, Marianne Busch</td>
</tr>
<tr>
<td></td>
<td>Section on Mobility Program</td>
<td>Manuel Clavel, Holger Schmidt</td>
</tr>
<tr>
<td></td>
<td>Section 6.2</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Section 6.3</td>
<td></td>
</tr>
<tr>
<td>V0.4</td>
<td>Updates of section 5</td>
<td>Carmen Fernandez, Fabio Martinelli</td>
</tr>
<tr>
<td>V0.5</td>
<td>Section 5.1, section 6.4</td>
<td>Carmen Fernandez, Fabio Martinelli</td>
</tr>
<tr>
<td>V0.6</td>
<td>Section 3 and 6 added. Inclusion of Appendixes</td>
<td>Carmen Fernandez, Francisco Moyano</td>
</tr>
<tr>
<td>V0.7</td>
<td>Updates on Sections 5.2, 5.3 and 7</td>
<td>Carmen Fernandez, Francisco Moyano</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Fabio Martinelli, Marina Egea,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Aljosa Pasic</td>
</tr>
<tr>
<td>V3.0</td>
<td>Approved my reviewers</td>
<td>Artsiom Yautisukhin, Fabio Massacci</td>
</tr>
</tbody>
</table>

## Document Review
<table>
<thead>
<tr>
<th>Date</th>
<th>Version</th>
<th>Reviewer</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>27-10-2011</td>
<td>3.0</td>
<td>Fabio Massacci (UNITN)</td>
<td>See report</td>
</tr>
<tr>
<td>4-10-2011</td>
<td>3.0</td>
<td>Artisom Yautisukhin (CNR)</td>
<td>See report</td>
</tr>
</tbody>
</table>
# Table of Contents

## TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
</tr>
<tr>
<td>7</td>
</tr>
<tr>
<td>10</td>
</tr>
<tr>
<td>12</td>
</tr>
<tr>
<td>13</td>
</tr>
<tr>
<td>14</td>
</tr>
<tr>
<td>14</td>
</tr>
<tr>
<td>15</td>
</tr>
<tr>
<td>16</td>
</tr>
<tr>
<td>16</td>
</tr>
<tr>
<td>17</td>
</tr>
<tr>
<td>18</td>
</tr>
<tr>
<td>19</td>
</tr>
<tr>
<td>20</td>
</tr>
<tr>
<td>21</td>
</tr>
<tr>
<td>21</td>
</tr>
<tr>
<td>21</td>
</tr>
<tr>
<td>21</td>
</tr>
<tr>
<td>24</td>
</tr>
<tr>
<td>24</td>
</tr>
<tr>
<td>26</td>
</tr>
<tr>
<td>26</td>
</tr>
<tr>
<td>27</td>
</tr>
<tr>
<td>28</td>
</tr>
<tr>
<td>29</td>
</tr>
</tbody>
</table>
7 ROAD-MAPPING ACTIVITIES ................................................................. 30

7.1 Two Main Crossing Research Themes of Major Interest .................................................. 32

7.2 Enabling Methodologies and Technologies to Enhance FI Trustworthiness ......................... 32

8 CONCLUSIONS .................................................................................. 35

REFERENCES ....................................................................................... 36

APPENDIX A: LIST OF ASSOCIATED PARTNERS ........................................... 37

APPENDIX B: EXTERNAL COMMUNITIES AND TECHNOLOGICAL PLATFORMS
LINKS AND DESCRIPTIONS .................................................................. 38
List of Figures

Figure 1 Onion Structure for NESSoS Actors .................................................................14
Figure 2 UMA Synergy Card- Front .............................................................................15
Figure 3 UMA Synergy Card- Reverse .........................................................................15
Figure 4 Geographical Distribution of Communities and Research Groups ...............22
Figure 5 Research Topics in Secure Service Engineering .............................................31
1 Executive Summary

The aim of this deliverable is the establishment of the strategy for the integration of the different communities in the area of secure service engineering. This integration will give us a result the creation of a long-lasting community in the area. The strategy considers the integration of agendas of the different actors involved in the area as well as the creation of a roadmap that will serve as the basis for a standing research in the area for the future.
2 List of Acronyms

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Full Form</th>
</tr>
</thead>
<tbody>
<tr>
<td>CBK</td>
<td>Common Body of Knowledge</td>
</tr>
<tr>
<td>E-RISE</td>
<td>European Technological Platform</td>
</tr>
<tr>
<td>ETP</td>
<td>European Technological Platform</td>
</tr>
<tr>
<td>FI</td>
<td>Future Internet</td>
</tr>
<tr>
<td>IAB</td>
<td>Industry Advisory Board</td>
</tr>
<tr>
<td>ICSE</td>
<td>International Conference on Software engineering</td>
</tr>
<tr>
<td>IFIP</td>
<td></td>
</tr>
<tr>
<td>JVRL</td>
<td>Joint Virtual Research Lab</td>
</tr>
<tr>
<td>NaLab</td>
<td>Network and Liaison advisory board</td>
</tr>
<tr>
<td>NESSI</td>
<td>Network of Excellence on Engineering Secure Future Internet Software Services and Systems</td>
</tr>
<tr>
<td>NESSoS</td>
<td>Network of Excellence on Engineering Secure Future Internet Software Services and Systems</td>
</tr>
<tr>
<td>PKI</td>
<td>Public Key Infrastructure</td>
</tr>
<tr>
<td>R&amp;D</td>
<td>Research &amp; Development</td>
</tr>
<tr>
<td>R &amp; I</td>
<td>Research &amp; Innovation</td>
</tr>
<tr>
<td>SDE</td>
<td>Service Development Environment</td>
</tr>
<tr>
<td>SDLC</td>
<td>Software Development Life Cycle</td>
</tr>
<tr>
<td>STM</td>
<td>Security and Trust Management</td>
</tr>
<tr>
<td>WG</td>
<td>Working Group</td>
</tr>
</tbody>
</table>
3 Introduction

One of the aims of NESSoS is the integration of research agendas for all the stakeholders in the area of secure service engineering. The integration of agendas will lead to the creation of a long-lasting community in the area of NESSoS that will consolidate the basis for the research to be done in a short-mid and long term.

In this deliverable we establish the integration strategies that we are going to follow for all the different actors that we are identified could be part of the NESSoS community. We follow an onion structure approach for these actors starting from the core partners of NESSoS as the most internal layer. Then, the integration follows for the outer layers such as associated partners, Industrial Advisory Board of NESSoS, Working Groups, Technological platforms and external research groups that collaborate with members of NESSoS.

A common feature for all the layers of actors is their inclusion in the community list of NESSoS, where events and news are published. The creation of collocated events with the main conferences in the area is something that we also consider as an integration strategy. Thus, this will be already realized for the ServiceWave conference (Poznan, October 2011) where the First NESSoS Industry seminar, Secure service engineering: from best practices to scientific excellence (and vice versa) will take place.

Another important aspect for achieving integration is the use of the specific tools that are being developed during NESSoS. Thus, the Mobility program tool will become of paramount importance for the integration of core partners whereas the Service Development Environment (SDE) and the Common Body of Knowledge (CBK) will at first be used for integration of core components and being expanded later on to the rest of the actors interested in NESSoS.

Besides the strategies we are establishing for integration, in order to obtain a long-lasting research community the NESSoS consortium is committed to the elaboration of research roadmaps in the area of secure service engineering. In this deliverable we will present the first of a series of research roadmaps that will set the basis for establishing a long-term research plan based on the common consensus from the different stakeholders in the area of secure software services and systems. In order to build the roadmap we used several sources. On one hand we used the initial deliverables on the State of the art of NESSoS and the outputs from a questionnaire sent to the core partners. On the other hand, we consider some common aspects with the roadmap being developed within the Effectsplus consortium. As a result, we identified a set of topics that we classified as common topics (threats to face, privacy, trust and Identity Management), topics for enabling methodologies and Technologies to Enhance FI Trustworthiness (Software Design Methodology, Security Requirement Engineering, etc) and crossing research themes (assurance and metrics, risk assessment, etc). In this deliverable we presented a short version of the document and attached the full version of it as part of this deliverable. This full version contains a short-term and long-term.

The structure of the deliverable is as follows. Section 4 outlines what is the motivation for creating a long-lasting research community. Section 5 shows an onion structure for classifying all the different actors involved in the area of secure service engineering and gives the different integration strategies for each of them. Section 6 describes the tools being developed within
NESSoS for the purposes of integration (i.e., Mobility Program, SDE and CBK). This section also describes NESSoS strategy for the organization of events being this a important pillar for integration. Section 7 gives a short version of the roadmap that is completed by an additional document containing the expanded version of it where all the topics are explained in detail. This long version also contains the NESSoS view of the area of secure service engineering that is used as a starting point for the roadmap.

This document also contains a series of appendixes. The first one contains a collection of the synergy cards of all the partners that have been designed in order to achieve internal integration among the core partners of NESSoS. The second one contains the description of the external groups and research communities that collaborate with NESSoS core partners.
4 Motivation for Creating an Integrated Agenda for Secure Service Engineering for the Future Internet Services

The area of secure software engineering services for the FI is of interest for different research communities. However, they address the problem from different points of view and approaches, remaining thus the research efforts in the area dispersed. The different communities that are involved and how they deal with the problem are as follows:

- **Software Engineering.** The software engineering community often leaves aside security in their developments. They usually consider it as a non-functional requirement and since their research is mainly concentrated in achieving functional requirements security is not considered from the beginning of the SDLC.

- **Security.** The security community has developed a considerable amount of mechanism such as security protocols or cryptographic schemes that are applied mainly on applications on run time and aspects that not take into account a holistic view. Thus, a relation in between security problems and security mechanisms should be stated more explicitly.

- **Formal methods.** The formal methods community concentrates its effort in developing methodologies for achieving assurance failing to provide these technologies to a larger scale available for practitioners. Thus, specific formal models for security properties are needed. Also, the compositionality problem should be addressed.

- **Services.** The ICT services community is becoming more and more interested in security aspects due to its relevance. In particular this community demands for:
  - Best and more rapid development techniques
  - Assurance methods to certificate security in services
  - More expressive languages for service composition and adaptation

In order to obtain a broadly and strong used approach for the development of secure services and systems the procedures followed by each of the communities mentioned above should be integrated. Thus, there is the need if integrating concepts, techniques and methods for the process of security requirements, architecture and design, programming techniques, assurance and risk and cost aware methods. All of them tested in application scenarios based on industrial problems.
5 Integration Strategy in the Area of Secure Service Engineering

The integration strategy of NESSoS will depend on the actors that are involved in it. We can distinguish the following actors:

a. NESSoS core partners
b. NESSoS associated partners
c. NESSoS IAB
d. External WGs (IFIP, ERCIM)
i. Main conference steerings committees (ICSE)
e. External EU projects (EFFECT+)
f. External ETPs (NESSI, etc.)
g. External research groups (list of single research groups to be contacted)
h. Creation of the NaLab

The strategy in order to fulfill integration will follow an onion approach, starting from the core partners of NESSoS and spreading towards all the other actors involved (see see Figure 1)
Thus, for each of them we will outline the steps required in order to achieve the integration.

5.1 Integration Strategy for NESSoS Core Partners

5.1.1 Identification of Synergies

The integration has to take place internally first, that is, among the partners in the NESSoS consortium. NESSoS partners work in different topics in the secure software engineering area and sometimes they are complementary or overlapping. In order to identify the synergies among the partners in the consortium we have distributed a Synergy Card where partners express their research topics and area of expertise as well as the current gaps they identify in their research together with the partners who work on those areas. Synergy cards of all the partners are at disposal of any partner interested in them at the BSCW repository. We do not plan to distribute them but to have them available for the use of partners as needed. An example of the card for UMA can be seen in Figure 2 and Figure 3.
Staff involved in NESSoS

<table>
<thead>
<tr>
<th>Name</th>
<th>Phone</th>
<th>Email</th>
</tr>
</thead>
<tbody>
<tr>
<td>Carmen Fernández</td>
<td>+34 952 134 186</td>
<td><a href="mailto:moggagol@lcc.uma.es">moggagol@lcc.uma.es</a></td>
</tr>
<tr>
<td>Gerardo Fernández</td>
<td>+34 952 134 185</td>
<td><a href="mailto:gerardo@lcc.uma.es">gerardo@lcc.uma.es</a></td>
</tr>
<tr>
<td>Francisco Moyano</td>
<td>+34 952 134 186</td>
<td><a href="mailto:moyano@lcc.uma.es">moyano@lcc.uma.es</a></td>
</tr>
<tr>
<td>J. Antonio Martín</td>
<td>phone</td>
<td><a href="mailto:jmartin@lcc.uma.es">jmartin@lcc.uma.es</a></td>
</tr>
<tr>
<td>Javier Cubo</td>
<td>phone</td>
<td><a href="mailto:cubo@lcc.uma.es">cubo@lcc.uma.es</a></td>
</tr>
</tbody>
</table>

Figure 2 UMA Synergy Card- Front

<table>
<thead>
<tr>
<th>Research topics</th>
<th>Current Gaps</th>
<th>Involved</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trust Management</td>
<td>Security Requirements Engineering</td>
<td>LMU, ATOS, UDE</td>
</tr>
<tr>
<td>Security Metrics</td>
<td>Security Problem Analysis</td>
<td></td>
</tr>
<tr>
<td>Security Requirements Engineering</td>
<td>Security Design</td>
<td>IMDEA, LMU, ATOS, UDE, INRIA</td>
</tr>
<tr>
<td>Service Composition and Adaptation</td>
<td>Secure Programming</td>
<td>CNR, IMDEA</td>
</tr>
<tr>
<td>Formal Methods</td>
<td>Model-Driven Approach</td>
<td>IMDEA, LMU, ETH</td>
</tr>
<tr>
<td>SaaS in Clouds</td>
<td>Secure Service Composition</td>
<td>CNR</td>
</tr>
</tbody>
</table>

Figure 3 UMA Synergy Card- Reverse

5.1.2 Joint Research
The core members of NESSoS are outstanding researchers in their corresponding area of expertise. Joint research among them could improve the overall quality and the advances could be enriched. Therefore, this becomes of paramount importance. The synergy cards described in Section 5.1.1 are a first step towards the identification of other partners within the consortium with whom collaboration is possible. These collaborations are aimed to lead to the increase the number of joint publications among NESSoS partners (the whole list of publications is available at http://www.nessos-project.eu/index.php?option=com_jresearch&view=publicationslist&Itemid=115).

Also, the NESSoS consortium celebrates regular general meetings where we discuss the research topics and how we are going to proceed for the short term, facilitating thus the interaction among partners.

5.1.3 Tools for the Integration of Core Partners

The tools for integration in NESSoS are

- Mobility program
- SDE. The Service Development Environment is an Eclipse-based, open source framework that provides an overview of available tools and their area of application
- CBK. The Common Body of Knowledge (CBK) helps to collect, structure, and integrate knowledge from the disciplines software engineering, service engineering, and security engineering

These tools are described in Sections 6.1, 6.2 and 6.3. The Mobility Program is exclusively an integration tool for the NESSoS core partners. However, the other two tools are expected to be available an open to associated partners first and interested researchers in general in the future, although at the moment they are also only available for NESSoS core partners.

5.2 NESSoS Associated Partners

The NESSoS consortium is supported for a group of experts in their respective areas that are associated partners for NESSoS. At the moment there are partners associated partners (see Appendix A) whom already showed their interest in NESSoS by writing supporting letters.

The process for developing our integration strategy with the associated partners comprises the following initial steps in order to carry out joint activities:

1. Addition to the community mailing list to keep them informed of the NESSoS ongoing activities since this list is used mainly for dissemination purposes.
2. Invitations:
   o To participate in NESSoS general meetings and organized events, such as workshops or panels.
   o To use the SDE and CBK tools (when their revision has been completed by NESSoS members).
3. Synergy cards distribution (excluding the part concerning participation in WPs). The use of the synergy cards as a strategy for integration among NESSoS core partners could be extended to associated partners.
Currently, associated partners are already included in the NESSoS community mailing list and some participated in the E-RISE event. Since the collaboration between core and associated partners is, in many cases, a matter of fact, the meeting opportunities in events organized by NESSoS can boost these collaborations, leading to the achievement of new outstanding research and technology transfer. The distribution of synergy cards could help a NESSoS partner to identify the actors working in the different research areas with common intersection in the area of secure software engineering services for the FI. This information constitutes a starting point to select a possible candidate that, for the nature of a problem addressed by the partner or for research-proximity reasons, can immediately collaborate with the partner.

5.3 **NESSoS Industrial Advisory Board**

The role of the IAB for the integration is many-fold. In industry there are many differentiated groups contributing to R&I that are target groups of the IAB for their integration in the community of NESSoS. A first group is composed of industrial experts whose area of work is basic research (but an industrial setting) and work in R&I departments. A second one is composed of industrial experts also working in R&I departments whose area of work is applied research or research driven by an innovation project. The third group is composed of those industry departments where employees are working directly for clients but who take innovative actions frequently in their daily work to provide a solution for the client. These three groups have already representation in the IAB.

Also, there are large industry-driven consortiums leading European innovation in secure software engineering and the FI with which the IAB chairman, Aljosa Pasic, is arranging meetings to be held in September/October 2011 to guarantee the contribution of NESSoS partners to the European mainstream innovation processes. For instance,

- [2011/10/18] Meeting with the Trust in Digital Life (TDL) Consortium. TDL is an initiative to set out a vision for trustworthy products relating to information and communications technology (ICT), including devices, applications, services, and infrastructures;
- [2011/10/10] Meeting with the leading European organization for the private security sector providers of technology solutions and services (EOS). EOS is open also to users and operators, representing all relevant domains of the economy (including ICT);
- [2011/29/09] Discussion with the EC-Directorate General for Information Society and Media about creating a European Innovation partnership for security.

The participation of ATOS in the FI-WARE project (that involves 20 major European ICT companies) is also enabling the integration of NESSoS partners’ interests with major ICT companies’ interests to support emerging FI services in multiple usage areas and standardization processes. In particular, in its WP9, FI-WARE is aimed to implement an
environment that will support both the Community of the developers that work on developing reference implementations of the FI generic enablers and the Community of developers that build Future Internet Applications on top of specific FI instances. The parts 1 and 2 of the integration strategy described in Section 5.2 for NESSoS associated partners would be offered as well to the new industrial partners. Up to now, we do not consider Synergy Cards useful for industrial partners given the large number of business areas in which they may be interested or may be competing instead of collaborating. However, synergy cards could be distributed to concrete groups within an industrial organization under request, e.g., to a research lab.

5.4 External Working Groups

The members of NESSoS are also members of very relevant Working Groups. These Working Groups celebrate events where we raise awareness about NESSoS and its objectives.

- ERCIM. NESSoS partners are members of several Working Groups of ERCIM. In particular
  - Security and Trust Management group of ERCIM. NESSoS has been presented in the last two workshops organized by this Working Group and it is also expected to be presented in the future at the Working Group meetings. Some partners are members of this WG (CNR, UMA, INRIA).
  - SERENE - ERCIM Working Group on Software Engineering for Resilient Systems (INRIA)
  - ERCIM Working Group on Software Evolution (INRIA)
- IFIP WG11.11 on Trust Management, where Fabio Martinelli is part of the steering committee (UMA is part of this WG as a member).
- IFIP Technical Committee (UMA is a member as the Spanish representative for it).
- European Organization for Security (EOS). ATOS is member of the board of directors
- Trust in Digital Life (ATOS is a member of the Advisory Board)
- Norwegian Computer Society where SINTEF leads several Working groups.
- The European Security Research and Innovation Forum (ESRIF) is divided into several WG being ATOS member of several of them as well for the European Public-Private Partnership for resilience (EP3R).
- Objet Management Group (OMG) and Open Geodata Consortium (OGC) to promote research results in industrial standards (SINTEF)

UDE is a member of the following WG:
- Founding member IFIP 2.9 Software Requirements
- EU expert group for software and service engineering
- Chair of GI-Special Interest Group (“Fachgruppe”) Software Engineering
• Chair of GI-Special Interest Group Software Product Management

ETH is a member of:
• IFIP working group 2.3 on programming methodology

5.4.1 Main Conferences Steering Committees

The core members of NESSoS are part of the steering committees of most of the main conferences in the different areas that NESSoS addresses such

• ESSoS. As this conference is the flagship event of NESSoS most of the steering committees are members of NESSoS (SIEMENS, KUL, UNITN). The integration with this conference is already a fact.
• ESORICS, EuroPKI, TrustBus, CRITIS (UMA is a member).
• Newly created conference POST (Principles of Security and Trust) (Fabio Martinelli), obtained though the merging of existing workshops as FAST.
• ESEC/FSE. The joint meeting of the European Software Engineering Conference and the ACM SIGSOFT Symposium on the Foundations of Software Engineering (INRIA)
• ACM/IFIP/USENIX International Middleware Conference (INRIA)
• ICST: International Conference on Software Testing, Verification and Validation (INRIA)
• Fabio Martinelli is also member of the SC of ETAPS (European Joint Conferences on Theory and Practice of Software)
• ESEC FSE Conference (Antonia Bertolino from CNR is a member).
• ACM ISSTA Conference (Antonia Bertolino is a member)
• MODELS: International Conference on Model Driven Engineering Languages and Systems (INRIA)
• AOSD: International Conference on Aspect-Oriented Software Development (INRIA)
• Security Measurements and Metrics (MetriSec) (SINTEF)
• International Symposium on Trustworthy Global Computing (TGC), 2011 (LMU)
• 11th International Conference on Web Engineering (ICWE 2011) (LMU)
• ICSE. In particular, we are negotiating with them the inclusion of a NESSoS workshop together with one of our regular meetings together with their conference in 2012 to be held in Zurich by ETH as host.

UDE is a member of the Steering Committee of the following conferences:

• International Conference on Computer Safety, Reliability and Security (SAFECOMP)
• International Conference on Software Product Lines
• International CAiSE Conference
• ServiceWave (European Conference on Software Services)
• International Workshop on Requirements Engineering: Foundation for Software Quality (REFSQ)
• International Workshop on Principles of Engineering Service ORiented Systems
• International Workshop on Variability Modelling in Software Product Lines (VAMOS)
• German Software Engineering Conference
• International Conference on Business Informatics
• Ubicomp Conference
• Pervasive Conference
• Percom Conference
• Conference on Tangible and Embedded Interaction,
• CHI Conference
• Conference on Mobile HCI Interaction
• Software Management Conference
• Member of the steering committee of several conferences, especially in the field of pervasive computing and human computer

ETH is a member of the following:

• Advisory committee for IEEE International Conference on Network and System Security (NSS), since 2008.
• ACM Symposium on Information, Computer and Communications Security (ASIACCS), since 2006.
• Steering committee and visiting faculty member for the Luxembourg International Advanced Studies in Information Technologies (LIASIT), since 2005.
• Founder and Steering Committee of ACM Workshop on Formal Methods in Security Engineering (FMSE), since 2003.

The overall strategy for the integration with these conferences is to include NESSoS by submitting papers on the topics of NESSoS or by creating satellite events or workshops within these main events for the specific areas of NESSoS, as it will happen with ServiceWave conference 2011, it happened with ESORICS (with FAST) and we are planning with ICSE.

5.5 External EU Projects
NESSoS core partners participate in other European projects, making in these cases easier for the projects know the advances and events that are taking place within NESSoS. In particular, we are in touch with other NoEs, such as SysSec by being subscribed in their community mailing list as well as they are subscribed to ours.
Special mention deserves the project Effectsplus. NESSoS is part of the Services and Cloud cluster, which is chaired by Fabio Martinelli (NESSoS coordinator). NESSoS participates actively in the meetings organized by this project by presenting it or presenting specific results. Also, the development of the research roadmap of NESSoS is taking very much into the account the outputs of the roadmap being developed at Effectsplus, as trust and security are crucial and horizontal topics for the secure service engineering area.
Besides that NESSoS members are also part of the consortium of other EU funded projects such as PICOS, PASSIVE, ASCENS, ANIKETOS or MASSIF.

5.6 Technological Platforms
NESSoS members are actively participating in technological platforms such

5.6.1 European

• Networked European Services and Software Initiative (NESSI). Most of the partners of NESSoS are members and part of the steering committee (ATOS and SINTEF).
• Networked & Electronic Media (NEM) Steering Board (SINTEF).
• Future Internet Public Private Partnership (FI PPP) Architectural Board (SINTEF)

5.6.2 National

• Iniciativa Española de Software y Servicios (INES). ATOS and UMA are members.
• Plataforma Tecnológica Española de Tecnologías para Seguridad y Confianza (eSEC). ATOS is member of the Executive Committee and UMA is a member.
• Security Research in Italy (SERIT)
• Asociación Multisectorial de Empresas de la Electrónica, las Tecnologías de la Información y Comunicación, de las Telecomunicaciones y de los contenidos (AETIC)

5.7 External Research Groups
NESSoS core partners collaborate with many research groups in their corresponding areas. We intend to make them aware of the advances and the work done in NESSoS by inviting them to join first the community list in order to keep them posted on NESSoS news through the newsletter. Thus, they can also join and be aware of the events organized by the consortium. The synergy cards can be also distributed among them in order to enforce the collaborations already started in the framework of NESSoS.

The map in Figure 4 shows the geographical distribution of the external links of the NESSoS partners. The specific links pert partner and the description of them can be seen in Appendix B.
Figure 4 Geographical Distribution of Communities and Research Groups

<table>
<thead>
<tr>
<th>ITALY</th>
</tr>
</thead>
<tbody>
<tr>
<td>Politecnico Di Milano</td>
</tr>
<tr>
<td>University of Pisa</td>
</tr>
<tr>
<td>University of Verona</td>
</tr>
<tr>
<td>CREATE-NET</td>
</tr>
<tr>
<td>University of Genoa</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SPAIN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Madrid’s security cluster  (INDRA, GMV, Grupo Gesfor,…)</td>
</tr>
<tr>
<td>University of Cadiz</td>
</tr>
<tr>
<td>INÉS</td>
</tr>
<tr>
<td>eSEC/AETIC</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>GREECE</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Foundation for Research and Technology - Hellas (FORTH)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>GERMANY</th>
</tr>
</thead>
<tbody>
<tr>
<td>Technische Universität Dortmund</td>
</tr>
<tr>
<td>Fraunhofer Institute for Software and Systems-Engineering - ISST</td>
</tr>
<tr>
<td>ITESYS Institut für technische Systeme GmbH</td>
</tr>
<tr>
<td>IT-Objects GmbH</td>
</tr>
<tr>
<td>Fraunhofer Institute for Secure Information Technology – SIT</td>
</tr>
<tr>
<td>Karlsruhe Institute of technology (KIT)</td>
</tr>
<tr>
<td>Institute of IT-Security and Security Law (ISL)</td>
</tr>
<tr>
<td>Microsoft EMIC</td>
</tr>
<tr>
<td><strong>FRANCE</strong></td>
</tr>
<tr>
<td>Institut Eurecom</td>
</tr>
<tr>
<td>University of Evry Val d’Essonne</td>
</tr>
<tr>
<td>Grenoble INP - INRIA Grenoble LIG</td>
</tr>
<tr>
<td><strong>UNITED KINGDOM</strong></td>
</tr>
<tr>
<td>University College London</td>
</tr>
<tr>
<td>City University London</td>
</tr>
<tr>
<td>British Telecom (BT)</td>
</tr>
<tr>
<td><strong>THE NETHERLANDS</strong></td>
</tr>
<tr>
<td>Vrije Universiteit Amsterdam</td>
</tr>
<tr>
<td><strong>BULGARIA</strong></td>
</tr>
<tr>
<td>The Institute for Parallel Processing at the Bulgarian Academy of Science (IPP-BAS)</td>
</tr>
<tr>
<td><strong>AUSTRIA</strong></td>
</tr>
<tr>
<td>Vienna Technical University</td>
</tr>
<tr>
<td><strong>SWEDEN</strong></td>
</tr>
<tr>
<td>Chalmers University</td>
</tr>
<tr>
<td><strong>TURKEY</strong></td>
</tr>
<tr>
<td>The National Research Institute of Electronics and Cryptology (TUBITAK-UEKAE)</td>
</tr>
<tr>
<td><strong>NORWAY</strong></td>
</tr>
<tr>
<td>University of Oslo</td>
</tr>
<tr>
<td>Gjøvik University College</td>
</tr>
<tr>
<td>University of Bergen</td>
</tr>
<tr>
<td><strong>LUXEMBURG</strong></td>
</tr>
<tr>
<td>University of Luxembourg</td>
</tr>
<tr>
<td><strong>SWITZERLAND</strong></td>
</tr>
<tr>
<td>IBM Zurich Research Laboratory</td>
</tr>
<tr>
<td>Zurich Information Security Center (ZISC)</td>
</tr>
<tr>
<td><strong>EUROPEAN GROUPS</strong></td>
</tr>
<tr>
<td>Trust in Digital Life</td>
</tr>
<tr>
<td>EOS</td>
</tr>
<tr>
<td>NESSI</td>
</tr>
<tr>
<td><strong>UNITED STATES</strong></td>
</tr>
</tbody>
</table>
5.8 Creation of a Network and Liaison Advisory Board (NaLаБ)

Chaired by Javier Lopez, the NaLAB aims to embody experience researchers world-wide (mainly not European) that have a significant role in the scientific community, as chairs of technical WG or coordinators of projects related to NESSoS. Our intention is to constitute this board with four experienced researchers. In order to do this the invitations to these researchers have been sent out and we are waiting for replies. This will contribute to the cooperation of these communities and NESSoS.

5.9 Long-Lasting View for Integration

One of the main goals of NESSoS is the integration of the research agendas of the different stakeholders in the area of secure software engineering. This integration will derive in a long-lasting research community that will overcome the current fragmentation of the different
communities. All the efforts for integration will be reflected in the Joint Virtual Research Lab (JVRL) that will integrate all the tools, data, human resources and the research knowledge derived from all the partners. This will serve as the basis for the cooperation within NESSoS and beyond the consortium. As first steps towards the creation of the JVRL the NESSoS consortium is working in the following aspects:

- Research in the area of secure Future Internet services is being carried out by the partners in the consortium. The main topics of research are (for more details on these research topics see [D6.1,D6.2,D7.1,D7.2,D8.1, D8.2, D9.1, D9.2, D10.1, D10.2]):
  - Security requirements engineering
  - Design of secure service architecture
  - Programming for secure and composable services
  - Security assurance for services
  - Risk and cost aware for the SDLC

- Creation of the Common Body of Knowledge. A first version is being created with contributions from NESSoS partners. For M12 it will be available only for partners but when the JVRL is available is expected to be widely for the whole research community (see Section 6.3 for more details).

- Integration of tools (see Section 6.1 for details)

- Contribution to education and spreading of excellence. The e-RISE event has been created for students to participate and test their tools. Also, the NESSoS summer school, FOSAD took place. We expect this summer school to last beyond the duration of NESSoS and be a consolidated summer school for new comers in the area of secure software engineering for future Internet services.

- In order to reduce the gap among industrial best practices and research some events are being held. For example, the first NESSoS industry seminar within the ServiceWave conference.
6 Tools for Supporting the Integration

6.1 Service Development Environment (SDE)

The SDE is an Eclipse-based, open source framework that provides an overview of available tools and their area of application. As for the case of NESSoS it gathers the tools that the partners have built on the past and that can be used in the future as a mean of integration of research among NESSoS partners.

The SDE allows developers to use integrated tools in a homogeneous way, re-arranging tool functionality in tool chains, and last but not least it enables users to stay on a chosen level of abstraction, hiding details of underlying tools.

All information about the SDE can be found at [http://www.nessos-project.eu/sde](http://www.nessos-project.eu/sde). This website is freely accessible and includes:

- a detailed tutorial about how to install and use the SDE and how to integrate plugins and to create tool chains,
- some screencasts of the SDE in action,
- a link to the SDE Eclipse update site together with the important information that the Eclipse Modeling version is required,
- a link to the SENSORIA ([http://www.sensoria-ist.eu/](http://www.sensoria-ist.eu/)), ASCENS ([http://www.ascens-ist.eu/](http://www.ascens-ist.eu/)) and NESSoS ([http://www.nessos-project.eu/](http://www.nessos-project.eu/)) projects in which the SDE is used as cornerstone for the integration and service-oriented usage of tools,
- a link to the SDE mailing list sde@maillist.ifi.lmu.de, which is mainly used for questions about the integration of new tools into the SDE (at the moment, members of the LMU answer to all messages, but everyone is free to join the mailing list in order to contribute to the SDE community),
- a bug tracking system for SDE, where everybody can view all tickets of known bugs or suggestions for improvements,
- code of the SDE that is located within a SVN (Subversion) repository, which can be anonymously checked out.

Tools that were used in the SENSORIA project can be found on this website as well; integration of tools related or developed within the scope of the NESSoS project are under construction and can be accessed through the CBK’s tool descriptions (see next chapter) that are currently NESSoS-internal (the necessary URL can be found in the section “Eclipse Update Site for SDE”).

The researchers can become acquainted with a new tool that is already integrated by straightforwardly installing and using it within the familiar workbench of the SDE. This leads researchers to get to know what others are investigating and it opens up new possibilities of collaboration due to the teamwork on building tool chains using tools from several partners.

Further information about the SDE can be found in deliverable D1.2 and D2.2.
6.2 Mobility Program

The mobility of fellows within the network is a mechanism that supports the integration of activities across various sites. It brings together researchers working on related topics; it drives knowledge exchange and knowledge generation through union and diversity. It increases the capability of joint cooperation among researchers.

Thus, the overall goal of the Mobility Program is to foster the integration of activities across the network partners. Each mobility action may pursue a different specific purpose (i.e., teaching short graduate, undergraduate, or industry-oriented courses in a different hosting organization; collaboration with industrial partners in carrying out industrial case studies; integrating different tools or validating them against large, complex, multi-facet scenarios; and so on), but all of them will contribute to increase the cohesion of the research ideas developed within the network and to promote the exchange of knowledge among the different partners. In particular, the following objectives are specifically addressed by the Mobility Program:

- To ease the mobility of the researchers within the consortium by providing adequate management support, especially for:
  - Medium-term exchange visits of PhD students, to integrate existing research infrastructure, methodologies and tools, and/or to carry out common case studies and applications.
  - Medium-term internships of PhD students with industrial partners, to reduce the gap among best practices and research.
  - Short-term, medium-term postdoctoral visits, to increase cohesion of research ideas, and promote exchange of knowledge.
  - Short-term, medium-term visits of industrial members at academic research partners (and vice versa), to foster industry-driven research and technology transfer.

- To create additional mobility positions within the consortium by leveraging on mobility programs set up by partners.

- To publicize the opening of mobility positions within the consortium, by creating and maintaining a web-based mobility information centre, with synergies and common interests, needs, and expertise among the partners. More specifically, the Mobility Portal (http://www.nessos-project.mbp) supports the Mobility Program in different ways. Basically, for simple visitors:
  - it provides up-to-date information about mobility actions already performed within the Mobility Program;
  - it graphically depicts, inside an annual calendar, the mobility actions already performed;
  - it provides up-to-date information about other mobility programs.

In addition, for those registrants in the Mobility Portal:
  - it provides an on-line application form to submit a request for a mobility grant;
it provides on-line access to their requests for grants, while they have not been yet accepted;

- it provides an on-line form to report about a mobility actions already performed. This report is automatically published, and available for visitors, in the Mobility Portal.

Last but not least, for the coordinators of the Mobility Program

- it provides on-line access to the pending requests for mobility grants, from which they can accept or reject the applications;

- it provides on-line access to the Mobility Portal's activity logs.

### 6.3 Common Body of Knowledge

The Common Body of Knowledge (CBK) ([http://www.nessos-project.eu/cbk](http://www.nessos-project.eu/cbk)) helps to collect, structure, and integrate knowledge from the disciplines software engineering, service engineering, and security engineering. It spans the field of secure software services and systems with respect to research findings as well as industry best practices. The main goal of the CBK is to support the creation of a long lasting research community on secure software services and systems. The CBK introduces mechanisms to collect knowledge based on Semantic MediaWiki technology, thus involving user participation. Quality-ensuring and enhancing processes support a more up-to-date, a more comprehensive, and a sustained CBK. A special ontology supports structuring the collected knowledge in a fairly automatic manner. This structure provides access to the CBK via a hierarchical taxonomy and represents a valuable instrument to discover gaps in practice and research. The knowledge stored in the CBK comprises the state-of-the-art in the field of engineering secure software and services. Moreover, the CBK establishes a common terminology that helps the community to find a common language of the different disciplines, and to define and use translations. Learning trails provide access to the CBK for a broader audience, practitioners and researchers in particular. When the CBK will be made available to the public in the second half of the NESSoS project, it will become a living document, i.e., it may be continually edited and updated by the community. The CBK comprises a handbook for the systems and software security engineer, in much the same spirit as the construction catalogues used in other engineering disciplines. See Deliverable 5.1 for more details.

The CBK supports the creation of a long-lasting integrated research community in different ways. Researchers and practitioners can use the CBK to find methods, tools, notations, and techniques based on different search criteria. This way, users can identify related work, detect research gaps and weaknesses, and find other researchers and practitioners that might be potential partners for future research projects, project applications, and joint research publications.
6.4 Organization of Events

A powerful tool to raise awareness on the NESSoS research topics and for consolidating the community is the organization of events, also in cooperation with other research communities. Indeed, scientific events are opportunities to discuss the recent advancement in the field as well as of creating consensus on the relevant topics to be further investigated (including prioritization of research activities). In particular, in the ambit of the NESSoS project, we consider several types of events:

- Official events organized by NESSoS where the NESSoS partners are involved and NESSoS research topics are discussed and presented (these events are also main outputs of the NoE).
- Events organized to create awareness of different research communities by NESSoS partners. In particular, with respect to the identified research communities mentioned previously, NESSoS has a plan to co-locate events as small-workshops (or NESSoS plenary meetings) together with the main events of those communities (security, software engineering, service engineering, formal methods, etc.). In particular, for the security community in Europe the main conference is ESORICS, for the service engineering one Servicewave/ISOC etc.
- Events jointly organized with other communities and/or EU projects in order to have mutual benefits and integrate the respective research activities.
- Events organized by NESSoS researchers not explicitly under the sponsorship of the NESSoS project, yet very useful for the consolidation of the research topics, the dissemination of new knowledge and thus sustaining the growth of the scientific community at large in the research topics of NESSoS.
7 Road-mapping Activities

A step towards the integration of research agendas is the production of research roadmaps. These roadmaps will set the basis for establishing a long-term research plan based on the common consensus from the different stakeholders in the area of secure software services and systems.

NESSoS roadmap in secure software services and systems is being developed in different phases. At a first stage we addressed the main topics of research considered by the NESSoS partners in their different areas of expertise, that coincide to some extent with the research topics of NESSoS for a short-mid term, i.e., the duration of the project. In order to do this we distributed a questionnaire to be answered by all the partners where they expressed how they foresee their research areas for the short-mid term and mid-long term period times. The methodology followed in order to elaborate the questionnaire was the same as the one used for the production of the roadmap by the EffectSPlus project [Wain11]. It was split into four core headings (changes, vision, challenges and gaps, and solutions). The answers were collected and analyzed giving as a result a set of common topics or research lines, that were the most mentioned by the partners, as key players in the Future Internet scenario. We will outline them and give a brief explanation in the following. They can also be seen in Figure 5. In the centre of the figure we have allocated the two major transversal research topics that are also main areas of research of NESSoS. Then, the methodologies and technologies that we identified will be crucial for the future in secure service engineering (again, these are the main of research topics of the NESSoS research activities). At the edges of the figure we identified the security properties that need to be addressed and the general threats that we will face in the case that research in the area is not performed.
Threats to face. In the Future Internet scenario, a new massive growth of cyber-crimes/cyber-attacks is expected. Future Internet will boost malware propagation through different kind of networks, either by moving physically (e.g. USB sticks, car-car, mobile devices) or by looking for communication gateways in the surroundings. This jump in communication capabilities along with the availability of more computing power, can be used by attackers to compromise resource constrained devices connected to the Internet, in order to access potentially dangerous resources and information sources. The implicit and explicit interdependences for offering IT services (often managed by different stakeholders) make it difficult to predict system behaviour as well as to enforce properly security policy and more general compliance to cross-border legislations. Prosumers (producers&consumers) creating and using services will lose control on their data (including the one regarding their personal sphere). Cyber-attacks are increasing in the scope and impact, targeting critical information infrastructures. There is also an increasing relationship between security and safety issues due to the proliferation of embedded system in our everyday life.

Properties to be ensured in FI. Several properties should be ensured for Future Internet: Compliance, Privacy, Trust, and Identity protection. These topics are currently becoming more and more important due to the increase of interoperability and heterogeneity concerns within the FI. It is worth to mention that location-privacy will be crucial in FI scenarios. Also,
the “right to be forgotten” is challenging. New schemas for identity management are required, since identity is emerging as an additional Internet layer with high impact within the FI. Also, trust management among boundaries will become of paramount importance in order to gain a tight integration of things, services and humans for an efficient and useful FI.

The need to embed security issues in the Future Internet service development life-cycle becomes evident. The next two sub-sections highlight the main research strands we consider worth of investigation in the mid-term.

7.1 Two Main Crossing Research Themes of Major Interest

**Security Assurance during SDLC**: Assurance will play a central role in the development of software-based services to provide confidence about the desired security level. Assurance will be treated in a holistic manner as an integral constituent of the development process (design for assurance), seamlessly informing and giving feedback at each stage of the software life cycle by checking that the related models and artefacts satisfy their functional and security requirements and constraints. Since the choice of appropriate assurance methods depends on several factors including the concrete application context and the desired level of assurance, this activity will cover a correspondingly broad range of assurance methods that jointly offer full development cycle support. Quantitative notions of security (including metrics) will allow to have systems able to trade-off among several requirements in a rationale way and considering multiple factors (including energy consumption for the protection mechanisms).

**Risk and Cost-aware SDLC**: It is hard to master risks and costs in service infrastructures, especially with the uprising of clouds and complex infrastructures. Some relevant goals are achieving traceability between risk and development models, managing evolving risks, and assessing risks at run-time. The definition and refinement of more precise economic security measures is necessary as well. As a matter of fact, the value of security solutions and their return on investment must be clearly demonstrated from a business oriented perspective. The value of the chosen security solutions has to be derived from the risk analysis. The net value of the investment must be derived by analysing the cost that comes with creating security solutions and implementing security measures. The integration of risk and cost analysis in the whole SDLC, and an extension of the overall approach towards execution time, are the necessary response to these needs.

7.2 Enabling Methodologies and Technologies to Enhance FI Trustworthiness

**Security Requirements Engineering**: The highly interconnected environment of the Future Internet, which mixes various infrastructure resources with application functionalities, inherits security risks from the classical Internet at the same time that it creates new and more complex
security requirements challenges, such as conflicts resolution amongst stakeholders interests or new types of security and privacy requirements, such as location-privacy. Other issues to address have to do with evolving requirements through the SDLC, having business-socio-economic requirements into account, and validating the completeness of the requirements.

**Secure Service Architectures and Design:** We need to increase the capability of designing secure software-based service systems for the internet of the future, to analyze security and ensure compliance of the underpinning architectures, and to include identification, assessment and improvement of design principles in order to enhance those architectures in terms of flexibility, modularity and composability, what will facilitate the integration of novel security services as the Future Internet scenarios evolve. Several approaches for modeling and developing architectures for SoA must be covered, including architecture design languages extended with security features as well as design approaches as design by contract (and its ‘relative” security by contract) and correct-by-construction (stepwise refinement). Other areas of interest that will be investigated for Future Internet paradigms (such as SaaS) include Model-driven architecture, Model-driven security, and other Model-driven development approaches.

**Security Support in Programming Environments:** This research area covers new programming platforms that deliver development and runtime environments for trustworthy application code to be executed in the complex application scenarios depicted by the Future Internet. We will also address language based security, as well as secure coding principles and practices. Research will both be based on language design and implementations, including middleware and run-time environment. Type systems, verifying compilers, support for run-time property verification and enforcement will be addressed here as well. Programming principles and constructs will be investigated in order to ease secure service development and composition for the new application scenarios. Code signatures as well as code instrumentations, aspect oriented and other composition techniques for security and secure execution environments are also in the scope of this area.

**Service Composition and Adaptation:** The integration and interoperability of services in order to tailor and enhance new services require adapting the service interfaces at different levels, including the semantic level. Other aspects to consider include assessing the trustworthiness of composition of services as well as and composing security measures.

**Run-time Verification and Enforcement:** Several levels of protection must be available. Thus run time enforcement of security properties is useful and must be further investigated. In this ambit, one of the most important gaps to overcome arises from the fact that security policies are typically formulated at high levels of abstraction whereas the monitors observe system events that are low-level. Model-driven approaches would be useful also in this context.

**Users Security Awareness:** users demand increasing the knowledge on the risks they are exposed to when using a service or a system. Changes in the context under which a service is running should be clearly informed to the user. This can be achieved by relying on good security usability mechanisms for end-users, and on friendly privacy controls.
**Security Management:** It is clear that secure services –especially the security features and related subsystems - should be supported with appropriate management support in order to observe the “quality of protection” in production systems at run time, and in order to implement the necessary measures for dealing with new threats and attacks, and possibly also with security incidents that require modification of the service implementation and/or its deployment environment.

**Autonomic Security:** FI services need to execute on a context, which is set up based on the service environment information. This would allow “autonomically” choosing different security mechanisms depending on certain levels of security required for a specific context. It also allows changing this context through the service execution life. For these purposes, new reasoners (decision making processes) need to be developed in order to intelligently exploit the service environment information, and thus, to predict security reconfiguration needs according to changes in this environment.
8 Conclusions

This deliverable has shown the integration strategies to be followed in order to build a long-lasting research community in the area of secure service engineering. The first step towards the description of these strategies has been the identification of this need for integration.

Then, the different strategies depending on the actors are introduced. The actors range from the core partners of NESSoS to the external communities and research groups that already collaborate with the NESSoS core partners. The latter list is included in an appendix due to length issues.

A first version of the research roadmap has also been included in this deliverable. The roadmap shows the topics identified by the NESSoS consortium as very relevant for the short-mid and mid-long term for the area of secure service engineering. The document containing the roadmap is structured in two parts. The first part is included in this document and contains a short version of the roadmap. A separate document containing the full version of the roadmap is included as part of this deliverable.
References

1. May 2011
Appendix A: List of Associated Partners

Ernesto Damiani, University of Milan, Italy
Claudia Eckert, SIT Fraunhofer, Germany
Jan Jurjens, TU Dortmund, Germany
Sokratis Katsikas, University of Athens, Greece
Bashar Nuseibeh, LERO, Ireland
Erik Poll, Radbound University Nijmegen, The Netherlands
Dave Sands, Chalmers University, Sweden
George Spanoudakis, City University, UK
## Appendix B: External Communities and Technological Platforms Links and Descriptions

<table>
<thead>
<tr>
<th>NESSOS partner</th>
<th>External communities</th>
</tr>
</thead>
</table>
| **ATOS**       | • Iniciativa Española de Software y Servicios (INES)  
• Plataforma Tecnológica Española de Tecnologías para Seguridad y Confianza (eSEC)  
• Asociación Multisectorial de Empresas de la Electrónica, las Tecnologías de la Información y Comunicación, de las Telecomunicaciones y de los contenidos (AETIC)  
• Trust in Digital Live (TDL)  
• European Organisation for Security (EOS)  
• Networked European Services and Software Initiative (NESSI)  
• Cloud Security Alliance (CSA) |
| **ETH Zurich** | • Zurich Information Security Center (ZISC)  
• IBM Zurich Research Laboratory  
• University of Verona  
• University of Luxemburg  
• Cryptography Research and Evaluation Committees (CRYPTREC) |
| **IMDEA**      | • Madrid’s security cluster  
• The Foundation for Research and Technology - Hellas (FORTH)  
• Politecnico Di Milano  
• Vrije Universiteit Amsterdam  
• Institut Eurecom  
• IPP-BAS  
• Vienna Technical University  
• Chalmers University  
• TUBITAK-UEKAE |
<table>
<thead>
<tr>
<th>Institution</th>
<th>Members</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• UC Berkeley - Bitblaze and Webblaze groups</td>
</tr>
<tr>
<td></td>
<td>• International Secure Systems Lab</td>
</tr>
<tr>
<td></td>
<td>• University of Wisconsin</td>
</tr>
<tr>
<td></td>
<td>• Georgia Tech University</td>
</tr>
<tr>
<td></td>
<td>• Carnegie Mellon University</td>
</tr>
<tr>
<td></td>
<td>• Stanford University</td>
</tr>
<tr>
<td></td>
<td>• Microsoft Research</td>
</tr>
<tr>
<td></td>
<td>• University of Bloomington</td>
</tr>
<tr>
<td>LMU</td>
<td>• Fraunhofer Institute for Secure Information Technology – SIT</td>
</tr>
<tr>
<td></td>
<td>• Institute of IT-Security and Security Law (ISL)</td>
</tr>
<tr>
<td>SINTEF</td>
<td>• University of Oslo</td>
</tr>
<tr>
<td></td>
<td>• Gjøvik University College</td>
</tr>
<tr>
<td></td>
<td>• University of Bergen</td>
</tr>
<tr>
<td>UDE</td>
<td>• Technische Universität Dortmund</td>
</tr>
<tr>
<td></td>
<td>• Fraunhofer Institute for Software and Systems-Engineering ISST</td>
</tr>
<tr>
<td></td>
<td>• IT-Objects GmbH</td>
</tr>
<tr>
<td>UMA</td>
<td>• University of Cadiz</td>
</tr>
<tr>
<td></td>
<td>• University of Pisa</td>
</tr>
<tr>
<td></td>
<td>• University of Evry Val d'Essonne</td>
</tr>
<tr>
<td></td>
<td>• University College London</td>
</tr>
<tr>
<td></td>
<td>• Grenoble INP - INRIA Grenoble LIG</td>
</tr>
<tr>
<td></td>
<td>• City University of London</td>
</tr>
<tr>
<td></td>
<td>• National University of Singapore</td>
</tr>
<tr>
<td></td>
<td>• Institute for Infocomm Research</td>
</tr>
<tr>
<td></td>
<td>• Tsukuba University</td>
</tr>
<tr>
<td></td>
<td>• Queensland University of Technology</td>
</tr>
<tr>
<td></td>
<td>• Dhirubhai Ambani Institute of Information and Communication Technology (DA-IICT)</td>
</tr>
</tbody>
</table>
External Communities Description

Madrid's security cluster

The Madrid’s security cluster is made of more than 40 organizations, among others INDRA, GMV and Grupo GESFOR. The main aims of the Madrid’s security cluster are:

- Help to promote Madrid as an international centre of excellence within the security market and ensure that its members remain at the forefront of innovation, stimulating and supporting the exchange of knowledge and collaboration and keeping them abreast of the latest advances in technology.
- Boost early demand projects with the aim of becoming a European leader and to turn the region into a trend-setter for the security sector.
- Provide access to a single geographic concentration of knowledge and experience at an international level, uniting all the actors of the value chain.

The Foundation for Research and Technology - Hellas (FORTH)

FORTH is the largest Greek State Research and Development Center. It consists of seven Institutes; the Institute of Computer Science (ICS) is one of them. In its twenty-year history, FORTH-ICS has established itself as an internationally known and highly competitive research institute, with modern infrastructure and a broad range of research, development, and educational activities in computer science, computer engineering and in communications. FORTH-ICS is staffed by approximately: 25 Ph.D holders, 70 engineers, 50 graduate student research assistants and 50 undergraduate student trainees.

Politecnico Di Milano

Politecnico di Milano is the largest Italian Technical University, with over 38.000 students in all areas of engineering, and over 1500 faculty members. It has a long tradition of research and teaching in all the domains of technology. The Dipartimento di Elettronica e Informazione (DEI) is the largest department of the university, providing research and education at all levels in the whole IT area. DEI has 180 faculty members and slightly short of 200 PhD students and postdoc researchers. DEI has been (and is) actively involved in a large number of European projects. The Performance Evaluation Laboratory (VPLab) leads the research in the dependability, security and performance areas. VPLab has been involved in several industrial, national and European research projects. In recent years, much of the research of VPLab has focused on intrusion detection, in particular anomaly detection, at both the host and the network level. The current research activities in the area of information security are focused on computer virology and automated forensic analysis.

Vrije Universiteit Amsterdam

The Vrije Universiteit (established 1880) is a private University located in the southern part of Amsterdam, The Netherlands. It has over 15,000 students studying in 12 faculties. The Computer Science Department is in the Faculty of Sciences and its staff consists of about 50 faculty members, several dozen postdocs and visiting researchers along with more than 40 Ph.D. students. The Vrije Universiteit Amsterdam (VU) is one of the leading European...
research centres in security, known for its work on intrusion detection and signature
generation for polymorphic, zero-day attacks.

Institut Eurecom
The Institut Eurecom is a non-profit research and teaching institute. EPFL and Telecom Paris
founded it in 1992. It specializes in communications and network engineering. Eurecom's
academic and research activities are organized in three departments: Mobile Communications,
Multimedia Communications and Corporate Communications. The Corporate Communications
department consists of six professors and assistant professors, two research engineers, a
dozen junior researchers and a number of master students. The security of mobile devices as
well as the monitoring and modeling of Internet threats are among its main areas of research.
The group has established an international reputation and its members are well involved in
their respective scientific communities.

IPP-BAS
IPP-BAS has a leading position among the scientific institutions in Bulgaria in the fields of
Computer Science, Scientific Computations, Supercomputing, Natural Language Processing
and Communications and Control. The staff of IPP-BAS consists of 108 people and the
research staff includes 62 people, working in 7 departments. The activities of IPP-BAS are
oriented mainly towards the creation and usage of advanced mathematical and information
technologies, analysis and development of tools, practices and regulations for network
monitoring, network security and with various Quality of Service (QoS) implementations.

Vienna Technical University
The Technical University Vienna is the largest technical university in Austria and among the
leading technical institutes in Europe. The university has more than 2,500 employees and is
divided into eight faculties with more than 60 institutes. The Secure Systems Lab, which will be
the direct partner for this project, is a joint research lab between the Institute of Information
Systems and the Institute of Computer Aided Automation. Currently, the lab is composed of
two faculty members, five PhD students, and nine Master's students. The research focus is on
applied computer security, with a recent emphasis on web security, malware analysis,
intrusion detection, and vulnerability analysis.

Chalmers University
Chalmers University of Technology was founded in 1829. More than 10,000 people, including
over 8,000 undergraduates, work and study in some of Chalmers' 16 departments. The
expertise of the Department of Computer Science and Engineering (CSE) ranges from
mathematical logic to applied industrial work with Intel. It combines scientific and engineering
approaches aiming at developing dependable and secure ICT systems. The Security group
has developed the link between two areas of computer science: programming languages and
computer security.

TUBITAK-UEKAE
The National Research Institute of Electronics and Cryptology (UEKAE), an affiliate of the
Scientific and Technological Research Council of Turkey, produces and applies scientific and
technological solutions with its qualified human resources and internationally accepted
infrastructure in the areas of information security, communications and advanced electronics.
UEKAE works on joint projects together with private sector companies and government
authorities by utilizing the TEMPEST, Acoustics, Common Criteria and Cryptographic Algorithm Design and Test Centers and Product Development, Electronic Warfare, Microelectronics and Optoelectronics departments. UEKAЕ, with 76% of its employees, consisting of researchers, contributes to universal science by incorporating the universities into the ongoing projects and encouraging its researchers for academic career development opportunities. UEKAЕ has the richest library in the areas of cryptology and information security in Turkey as well.

UC Berkeley - Bitblaze and Webblaze groups
The Bitblaze group is specialized in the Binary Analysis for Computer Security (http://bitblaze.cs.berkeley.edu/) and the Webblaze one aims to design and develop new techniques and architectures for securing the Web (http://webblaze.cs.berkeley.edu/)

International Secure Systems Lab
The International Secure Systems Lab is the union of five systems security research labs and was originally founded in 2005 at the Technical University of Vienna. As of 2008, the Secure Systems Lab has become international and was initially distributed over three geographical locations including the Institute Eurécom in the French Riviera and the University of California, Santa Barbara. In 2010, Ruhr University in Bochum in Germany joined the iSecLab family, and in 2011, Northeastern University came on board. Lab members collaborate closely, apply for joint funding, share data, exchange ideas, and have fun together. iSecLab encourages and supports student and faculty mobility within the labs. The research focus is on applied computer security, with a recent emphasis on web security, malware analysis, intrusion detection, and vulnerability analysis.

University of Wisconsin
The group leaded by Somesh Jha works in security and software engineering topics.

Georgia Tech University
The group leaded by Wenke Lee's focuses its research interests in systems and network security, applied cryptography, network management, and data mining.

Carnegie Mellon University
The group lead by David Brumley's is interested in all areas of computer security, applied cryptography, program analysis, compilers, and verification. There is another group lead by Adrian Perrig’s, which research interests focuses on networking and systems security, security for mobile computing, sensor networks, human interfaces for security, networking, operating systems, and applied cryptography.

Stanford University
The group coordinated by John C. Mitchell at Standford University focuses its research interests on computer security: access control, network protocols, privacy, software systems, and web security. Programming languages, type systems, object systems, and applications of mathematical logic to computer science.
Microsoft Research
The Microsoft Research security group lead by Helen Wang conducts broad security and privacy research in systems including mobile systems, networking including wireless networking, and human computer interfaces. Its mission is to advance the state-of-the-art and solve pressing real-world problems to impact MS products as well as the entire computing industry.

University Bloomington
XiaoFeng Wang's group at Indiana University Bloomington currently focuses its research interests on three main topics: Privacy Protection in Human-Genome Research, Cloud and Web Security and Software and System Security.

University of Cadiz
The group coordinated by Guadalupe Ortiz at University of Cadiz (Spain) is interested in aspect-oriented techniques, model-driven extra-functional properties and quality of service development, context-awareness and adaptation in mobile devices, integration of complex-event processing in service-oriented architectures.

University of Pisa
The group lead by Antonio Brogi at University of Pisa focuses its research interests in service-oriented computing, coordination and adaptation of software elements and design of programming languages.

University of Evry Val d'Essonne
The group lead by Pascal Poizat focuses its research interests in model-based (formal) techniques for the composition, coordination and adaptation of software.

University College London
Research interests: scalability of architectures for large-scale software systems, and validation of mobile, context-aware adaptive systems for ubiquitous computing.

Grenoble INP - INRIA Grenoble LIG
The group lead by Gwen Salaün focuses its research interests in formal techniques and tools, process algebras, concurrent and distributed systems, specification and verification, composition and adaptation of software components and services.

City University London
The group lead by George Spanoudakis focuses its research interests in service-based systems engineering and software systems security.

National University of Singapore
Research interests: scalability of architectures for large-scale software systems, and validation of mobile, context-aware adaptive systems for ubiquitous computing.
**Iniciativa Española de Software y Servicios (INES)**

INES (Iniciativa Española de Software y Servicios) is the Spanish Technology Platform for Software Systems and Services. INES is a scientific-technological network whose mission is to increase the Spanish industry competitiveness through cooperation between all the stakeholders involved: companies, technology centres, universities, etc.

**Plataforma Tecnológica Española de Tecnologías para Seguridad y Confianza (eSEC) and Asociación Multisectorial de Empresas de la Electrónica, las Tecnologías de la Información y Comunicación, de las Telecomunicaciones y de los contenidos (AETIC)**

eSEC is the Spanish Technological Platform for Security, Trust and Dependability. It is composed by more than 220 entities, including industries, researchers and users. Main objective of eSEC is to promote real competitiveness of the Spanish ICT security industry thought dialog and cooperative research and innovation. eSEC is secretariat by AETIC which is the Spanish Electronics, Information Technology and Telecommunications Industries Association

**Trust in Digital Life (TDL)**

The Trust in Digital Life Consortium is a new initiative that aims, over the course of two years, to set out a vision for trustworthy products relating to information and communications technology (ICT), including devices, applications, services, and infrastructures. Central to this vision shall be recognition of the importance of the rule of law, security, and privacy and other core democratic freedoms in contributing to trustworthiness. The TDL Partnership will translate this vision into an agenda for research and innovation, placing particular emphasis on transparency and accountability. In the process, the TDL Partnership will coordinate with other initiatives as it takes an inventory of emergent digital technologies that can be combined to implement the vision, and it will engage in a broad dialogue. By presenting scenarios, or use cases, Members will illustrate how combinations of trustworthy ICT-related products can give effect to specific public policy goals.

**European Organisation for Security (EOS)**

European Organization for Security (EOS) groups the private-security-sector main actors, coming from 13 different European countries: technology solutions and managed services providers (ICT, defence, civil security, energy, transport, finance, services and research), as well as users and operators. EOS aims at developing a consistent European Security Market and a sustainable European Security Model that satisfies political, social and economic needs through the efficient use of budgets and the implementation of available solutions in priority areas.

**Networked European Services and Software Initiative (NESSI)**

European Technological Platform, software and services. Atos through Atos Research and Innovation has the vice presidency of the joint management (NESSI Board ) and the steering committee. Atos is the leader of European Union member states and also national software and services platforms activities. Atos is also leader of work groups “Trust, Security and Dependability”, “eHealth” and “Semantic Technologies”.

**Cloud Security Alliance (CSA)**
The Cloud Security Alliance is a non-profit organization formed to promote the use of best practices for providing security assurance within Cloud Computing, and provide education on the uses of Cloud Computing to help secure all other forms of computing. The Cloud Security Alliance is comprised of many subject matter experts from a wide variety disciplines, united in our objectives:

- Promote a common level of understanding between the consumers and providers of cloud computing regarding the necessary security requirements and attestation of assurance.
- Promote independent research into best practices for cloud computing security.
- Launch awareness campaigns and educational programs on the appropriate uses of cloud computing and cloud security solutions.
- Create consensus lists of issues and guidance for cloud security assurance.

**Technische Universität Dortmund**

The software Engineering (LS 14), belonging to the department of Computer Science, is led by Jan Jürjens. Its interests comprise engineering of secure software, model-based security, and security and compliance.

**Fraunhofer Institute for Software and Systems-Engineering ISST**

This ISST group is led by Jan Jürjens. Its interests comprise engineering of secure software, model-based security, and security and compliance.

**ITESYS Institut für technische Systeme GmbH**

ITESYS Institute for Technical Systems is a company in the area of information and communication technology. ITESYS has long-term experience in specifying, developing and automatically testing technical systems that are critical w.r.t. safety and security.

**IT-Objects GmbH**

IT-Objects is a company that offers customized services within the IT branch, e.g. software development and consulting. IT-Objects is a partner of the international research project PICOS (Privacy and Identity Management for Community Services) on the European level with the main focus on mobile communication.

IT-Objects undertakes tasks in the areas of requirements analysis, architectural development, and implementation.

**Fraunhofer Institute for Secure Information Technology – SIT**

To further develop the Fraunhofer - SIT competencies and to be able to accompany the research developments in the various IT security areas the Institute is organised in research fields, that are dedicated to different thematical:

- Embedded Security and Trusted OS
- Information Assurance
- Network Security and Early Warning Systems
- Security Modeling and Validation
- Secure Mobile Systems
- Ambient Security
- Application and Process Security
- Secure Services and Quality Testing
- Transaction and Document Security

Contact: director of the Fraunhofer – SIT, Prof. Claudia Eckert.

Institute of IT-Security and Security Law (ISL)
The Institute of IT-Security and Security Law (ISL), which is part of the University of Passau is characterised by its interdisciplinary focus on computer science, law and economics. For the first time, the technical and economical aspects of IT security are extended to the dimension of law. The focus of the Institute is the synergy between theory and practice as well as research and industry.

Contact: Chairman of the institute, Prof. Dr. Joachim Posegga

University of Oslo - Department of Informatics, Department of Media and Communication and Norwegian Research Center for Computers and Law
The Distributed Multimedia Systems (DMMS) Research Group at the Department of Informatics is aiming to improve future networks and middleware for advanced multimedia applications. Multimedia does not only mean audio and video, but also sensor data of any kind. We investigate context-aware and self-adapting solutions for transmission, distribution and management of (multimedia) data. Our current research is centered around Home Care (Multimodal Event Systems and Applications), Future Internet (Autonomic Networks and Autonomic Systems), Future Media (Content Distribution) and Emergency and rescue operations (Mobile Data Management Systems).

Media Innovations explores how changing technologies and changing modes of usage and engagement with media bring about media innovation and transformation of the media sector. Users of digital media are becoming increasingly more active as producers (and re-distributors) of content, contributing to new services, new genres, new social constellations and new business models. By emphasizing how interrelations between media technology and users contribute to drive innovation, Media Innovations will provide a framework for studying change that enables a deeper understanding of the ongoing developments, and the possibilities and challenges this involves for individuals and society.

From the very beginning, the NRCCL has been internationally oriented. Today the NRCCL is established as one of the leading international institutions in the area of ICT-related law. With an academic staff of approximately 30 full-time professors and the researchers, the NRCCL has solid expertise in all major areas. A basis for research issues is legal technology, including but not limited to legal information systems and knowledge based systems.

Gjøvik University College - Norwegian Information Security laboratory (NISlab)
NISlab is part of the Faculty for Computer Science and Media Technology. The group conducts international competitive research in several areas of information security,
supervises Ph.D. research projects in this field and teaches courses in information security at the master and bachelor level.

University of Bergen - Department of Information Science and Media Studies

The department studies, with varied approaches and methods, information and communications technologies, their historical, actual and potential functions in relation to individuals, groups, organizations, institutions and society, and their aesthetic aspects and subject matter. The multi-faceted research carried out at the department reflects this. A number of new study options have been developed based on the research. The department offers a number of theoretically and practically oriented studies in addition to the traditional academic subjects in the field of information science and media studies.

Institute for Infocomm Research

The mission of the Network Security Group in I2R is to help address the different threats (e.g. gaining illegal profits, destroying a country's economy, paralyzing a business competitor's service) that affect the Internet through world-class research and manpower training on network security. Its main research areas are the following: applied cryptography, mobile IP security, secure Internet applications, smart grid security, and wireless sensor network security. At present, its research is focused on the protection of smart grid infrastructures (project SecSG - Cyber Security for EV Ecosystem in Smart Grid) and on scalable storage security systems (project SecDC - Secured Large Scale Shared Storage System).

The main contact is Dr. Jianying Zhou.

Tsukuba University

Queensland University of Technology

UMA: TBC

Dhirubhai Ambani Institute of Information and Communication Technology (DA-IICT)

Beyond offering a series of security courses that aim to teach Indian students about how to protect information and communications technologies, the Security Group of DA-IICT carries out research on security protocols, cryptographic primitives, access control, and formal verification. In particular, the Security group is currently applying their expertise on the following two areas: security proofs and multidisciplinary evaluation for dynamic hierarchical key assignment schemes, and security and privacy infrastructures for "Internet Of Things" scenarios and applications.

The main contact is Dr. Manik Lal Das

University of Sao Paolo

The LSD (Laboratorio de Seguridad Digital) at the University of Sao Paulo includes professors, PhD students, postdocs and external researchers. Amongst other goals, it aims at students training and the development of new technologies in the information security area in Brazil, encouraging the development of secure applications, and fostering the improvement and advanced training of its members. The main goal of LSD is to be a centre of excellence in Brazil aiming at the development of information security applications. Their research particularly concentrates on the area of Applied Cryptography. The main contact is Prof. Routo Terada.

Zurich Information Security Center (ZISC)

The Zurich Information Security Center (ZISC) began its operation in September 2003, bringing together academia and industry to carry out research and education in information security.
IBM Zurich Research Laboratory
The IBM Zurich Research Laboratory was a member of the ZISC consortium until August 2011. The security group is doing research on formal verification tools, identity governance, Internet transaction security, security policies, and cloud computing security.

University of Verona
The information security research group is working on formal methods for information security, including the modeling and verification of security protocols that are relevant for FI applications.

University of Luxemburg
The Security and Trust of Software Systems group does research on formal modelling and reasoning about real-world security problems and trust issues.

Cryptography Research and Evaluation Committees (CRYPTREC)
This is a project of the Japanese Government for the evaluation and monitoring of cryptographic techniques and protocols with the aim of assuring e-Government security.

BT
British telecom is the main actor in secure telco service research including cloud and grid computing. CNR has a lost standing research collaboration with Dr. Theo Dimitrakos (theo.dimitrakos@bt.com) established through the coordination of joint research communities and also through the exchange of people among the two research groups.

University of Genoa
Alessandro Armando (Armando@dist.unige.it) at the University of Genoa works on automated verification of secure software and services with advanced model checking techniques. Alessandro is also working part time at FBK in Trento as security group leader.

Karlsruhe Institute of technology (KIT)
Alexander Pretschner (alexander.pretschner@kit.edu) group on advanced techniques for distributed usage control as well as testing techniques for service architecture.

CREATE-NET
Create-net is an active private research centre in Trento, with a strong background on networking and pervasive computing also with a group operating in security with experience on running EU projects. Giovanni Russello is the main contact (giovanni.russello@create-net.org).

Microsoft EMIC
Microsoft EMIC is the main innovation centre of Microsoft in Europe with strong interest in security. Several partners of NESSoS collaborated with them in previous EU projects as CONSEQUENCE. Joris Claessens and Alexey Orlov are potential point of contact.