Network of Excellence

D4.3 Part I:
Final Report on the Cutting-Edge Activities, Alignment and Integration with Relevant European and International Activities and Release of the Research Roadmap
Abstract

This deliverable reports an update of D4.2 on the activities carried out within the NESSoS consortium in order to achieve integration with other communities that work also on the area of secure service engineering.

Keyword list

Future Internet, Software and Service Engineering, Security, Integration activities, events, Roadmap
### 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>Table of Contents</td>
<td>Carmen Fernandez</td>
</tr>
<tr>
<td>V0.2</td>
<td>Sections 2, 3, 4 and 5</td>
<td>Carmen Fernandez, Francisco Moyano, Pablo Najera (UMA)</td>
</tr>
<tr>
<td>V0.3</td>
<td>Comments by reviewers addressed</td>
<td>Carmen Fernandez (UMA)</td>
</tr>
<tr>
<td>V3.0</td>
<td>Approved by the reviewers</td>
<td>Carmen Fernandez, Francisco Moyano, Pablo Najera (UMA)</td>
</tr>
</tbody>
</table>
# Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>TABLE OF CONTENTS</td>
<td>3</td>
</tr>
<tr>
<td>LIST OF FIGURES</td>
<td>5</td>
</tr>
<tr>
<td>LIST OF TABLES</td>
<td>5</td>
</tr>
<tr>
<td>LIST OF ACRONYMS</td>
<td>6</td>
</tr>
<tr>
<td>EXECUTIVE SUMMARY</td>
<td>7</td>
</tr>
<tr>
<td>1 INTRODUCTION</td>
<td>8</td>
</tr>
<tr>
<td>2 JOINT RESEARCH ACTIVITIES WITHIN THE NESSoS CONSORTIUM</td>
<td>9</td>
</tr>
<tr>
<td>2.1 Collaborations within NESSoS Core Partners</td>
<td>9</td>
</tr>
<tr>
<td>2.2 Collaborations with Associate Partners</td>
<td>25</td>
</tr>
<tr>
<td>3 NESSoS ACTIVITIES FOR ACHIEVING INTEGRATION</td>
<td>27</td>
</tr>
<tr>
<td>3.1 NESSoS Meetings</td>
<td>27</td>
</tr>
<tr>
<td>3.2 Flagship Event: ESSoS Conference</td>
<td>28</td>
</tr>
<tr>
<td>3.3 Participation in Activities with Other Communities</td>
<td>29</td>
</tr>
<tr>
<td>3.4 Other Events</td>
<td>37</td>
</tr>
<tr>
<td>3.5 Education and Training Activities</td>
<td>38</td>
</tr>
<tr>
<td>3.6 Roadmapping Activities</td>
<td>38</td>
</tr>
<tr>
<td>4 REPORT ON THE NALAB ACTIVITIES</td>
<td>41</td>
</tr>
<tr>
<td>5 CONCLUSION</td>
<td>42</td>
</tr>
</tbody>
</table>
List of Figures
Figure 1 Joint Research ................................................................. 21
Figure 2 Joint Publications ......................................................... 22
Figure 3 Joint Project Proposals .................................................. 23
Figure 4 Joint Organisation of Events .......................................... 24
Figure 5 Joint PhD Supervision .................................................. 25
Figure 6 Quantification of Addressed Topics .............................. 37
Figure 7 Roadmap Topics ............................................................ 39

List of Tables
Table 1-CNR Collaborations ....................................................... 10
Table 2-ATOS Collaborations ..................................................... 11
Table 3-ETH Collaborations ....................................................... 12
Table 4-IMDEA Collaborations ................................................... 13
Table 5-INRIA Collaborations .................................................... 14
Table 6-KUL Collaborations ....................................................... 14
Table 7-LMU Collaborations ...................................................... 15
Table 8-SIEMENS Collaborations ............................................. 16
Table 9-SINTEF Collaborations .................................................. 17
Table 10-UDE Collaborations ..................................................... 18
Table 11-UMA Collaborations .................................................... 19
Table 12-UNITN Collaborations ................................................. 20
### List of Acronyms

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FI</td>
<td>Future Internet</td>
</tr>
<tr>
<td>SDLC</td>
<td>Software Development Life Cycle</td>
</tr>
<tr>
<td>WG</td>
<td>Working Group</td>
</tr>
</tbody>
</table>
Executive Summary

This deliverable is an update of [D4.2_I]. It describes the activities carried out by NESSoS in order to achieve the integration of research agendas in the area of secure service engineering. As in previous editions, this deliverable is divided into two parts. The first part, which is the current document, describes the activities carried out by the members of the consortium. The activities of NESSoS are twofold. On one hand, we consider the activities carried within the NESSoS consortium, including associate partners, and on the other hand, the activities organised with other communities in order to achieve a broader integration with the whole research community.

The activities performed within the NESSoS consortium have been classified into different categories: joint research, joint publications, joint project proposals, joint organisation of events, and joint PhD supervision. The analysis performed on joint activities within the NESSoS core consortium shows that collaborations are well established and part of the research in NESSoS. Every partner collaborates in different activities with at least three other partners. This is reflected also in the number of joint publications, which has increased during the third year to 16.1% (see [D12.5]).

We describe in this deliverable all the events we have participated together with other communities (FIA, CSP, APF, etc.). We can see that we have been present in most of the relevant events related to NESSoS research, explaining the NESSoS proposals for research in the future. It is interesting for us to analyse whether the events we collaborate with are in the areas of research that NESSoS proposes in its roadmap. This analysis shows that we have covered in the topics of the events we have organised most of the topics that are interesting for research according to our roadmap. Definitely, we have covered more topics than last year.

Undoubtedly, one of the main achievements of NESSoS on the integration of agendas has been the creation of the IFIP WG11.14 on Secure Engineering. This WG was proposed by NESSoS partners and will be chaired by Fabio Martinelli. It will guarantee that the effort started by NESSoS on fostering research in secure service engineering will continue beyond the end of the project through this WG.

We have also described the activities performed together with the members of the NALaB. During the third year of the project we have invited them to comment and contribute to our research roadmap. These interactions have provided us with very useful comments that are reflected in the final version of the roadmap [D4.3_II].

The second part of the deliverable describes the final version of the NESSoS roadmap, which is presented in a separate document due to its length.
1 Introduction

One of the NESSoS goals is the creation of a long-lasting research community in the area of secure service engineering that lasts beyond the life of NESSoS.

Traditionally, most of the researchers working on the different aspects involved in the area of secure service engineering have worked in an isolated way. Thus, the first step towards the creation of the community is the identification of existing gaps and the design of a strategy that helps mitigating the fragmentation on the research done so far.

The first step that the NESSoS consortium took towards the mitigation of this fragmentation started from within the project. Different collaborations started during the first year. Moreover, the number of collaborations has grown during the lifetime of the project. Thus, we can say that every partner has established collaborations in different research activities with at least two other partners. We classified the type of activities that we analysed into different categories: joint research, joint publications, joint project proposals, joint organisation of events, and joint PhD supervision.

Apart from the collaboration within the NESSoS consortium the project has established relationships with relevant communities. Most of these relationships have resulted in the participation in important events such as the Future Internet Assembly (FIA) or Cyber Security and Privacy Forum (CSP), among others. We can highlight the creation of the IFIP WF11.14 on Secure Engineering as a very relevant relationship established as a consequence of the efforts of NESSoS for achieving integration. The creation of this new WG under the auspices of IFIP will ensure that the efforts started by NESSoS on the establishment of a community will remain after NESSoS is finished.

We have performed an analysis that compares the topics relevant to the events where NESSoS has participated to the topics that NESSoS consider important for research. We have observed that we have approach in our events practically all the topics that the consortium identified as important in secure service engineering.

An important tool to set up the layout of an integrated research in the future is the development of a research roadmap. In a separate document we have presented the NESSoS research roadmap on secure service engineering. This roadmap has the potential to set the basis for research in the coming years by highlighting which are the most important topics that need to be considered for research in the area of secure service engineering according to the NESSoS community.

This document is organised as follows. Section 2 describes the activities carried out within the NESSoS consortium, including associate members, whereas Section 3 describes the other type of activities carried out with other communities. The analysis that compares the topics of the activities where NESSoS participated and the NESSoS research topics is also described in this section. NESSoS NaLAB’s activities are described in Section 4 and Section 5 concludes the document and outlines the future work.
2 Joint Research Activities within the NESSoS Consortium

A fundamental part of the integration of research agendas is the activities and research that are carried out within the NESSoS consortium. This set of activities can be classified into different categories:

- Joint research and publications
- Joint project proposals
- Joint organization of events
- Joint PhD supervision

In Section 2.1 we will analyse the activities carried out by each partner according to the above classification and in Section 2.2 we will describe the activities carried out with associate partners.

2.1 Collaborations within NESSoS Core Partners

In this section we describe the peer-to-peer collaborations

<table>
<thead>
<tr>
<th>CNR</th>
</tr>
</thead>
</table>

**Joint research and publications**
- Joint publication entitled ‘PERSONA: a personalised data protection framework’ → ATOS, UNITN and Technical university of Eindhoven
- Joint publication on ‘A Toolchain for Designing and Testing XACML Policies’ → LMU
- Joint publication ‘A tool for secure service orchestration’ → UMA
- Work in Progress on ‘UWE - XACML toolchain’ → LMU
- Work in Progress on a survey on synthesis mechanism → INRIA
- Planned joint research to use SI* threat modelling with the attack graph approach from UDE
- Collaboration in ITEA2 DIAMONDs project → SINTEF

**Joint Project Proposals**
- Funded proposal in Call 10 on Confidential and Compliant Clouds → ATOS

**Joint organization of events**
- 7th International IFIP WG 11.11 on Trust Management, June 2013 → UMA
- IFIP/NESSoS/ANIKETOS/ChoREOS Spring School On ‘Trustworthy Services and Systems’ → ATOS, INRIA, UMA.
- FIA’13 session in Dublin on ‘How far do we have to go to make the Internet secure?’ → UMA. This session was organized in conjunction with projects BIC and Seccord.
- Session on privacy by design at Computers, Privacy and Data Protection (CPDP’13) → SIEMENS and ATOS.
- FIA pre-workshop on Future Internet Services → INRIA, UMA (in cooperation with ANIKETOS and CHOREOS projects).
• Co-organization of QASA’13 workshop, affiliated with ESORICS, September 2013 → IMDEA
• Organization of the second ESSoS doctoral symposium in Paris on February, 27th 2013 → UDE

The collaborations of CNR can be seen in Table 1.

In the following the collaborations that happen among more than three partners are identified with the same colours in the tables. Where the abbreviations stands for the following:

• **JR** stands for that joint research is being carried out
• **JP** If the joint research produced joint publications
• **JPP** means joint project proposal
• **JOE** stands for joint organization of events
• **JPhD** for joint PhD supervision

Same colour ticks in a column mean that the collaboration is happening among the partners where the tick is.

<table>
<thead>
<tr>
<th></th>
<th>JR</th>
<th>JP</th>
<th>JPP</th>
<th>JOE</th>
<th>JPhD</th>
</tr>
</thead>
<tbody>
<tr>
<td>ATOS</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>ETH</td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IMDEA</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>INRIA</td>
<td>✓</td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>KUL</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>LMU</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SIEMENS</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>SINTEF</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>UDE</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>UMA</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>UNITN</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*Table 1-CNR Collaborations*

**Joint research and publications**

- Joint publication entitled ‘PERSONA: a personalised data protection framework’ → CNR, UNITN and Technical university of Eindhoven (TUE)
- Joint publication entitled ‘Verification of ATL Transformations Using Transformation Models and Model Finders’ → INRIA
- Joint publication entitled ‘Checking Model Transformation Refinement’ → INRIA
- Submitted journal paper entitled ‘A Model-Driven Methodology for Developing Secure Data-Management Applications’ to Transactions on Software Engineering (TSE) → ETH, IMDEA

**Joint Project Proposals**

- Funded proposal in Call 10 on Confidential and Compliant Clouds → CNR
Joint organization of events
- IFIP/NESSoS/ANIKETOS/ChoREOS Spring School On 'Trustworthy Services and Systems' → CNR, INRIA, UMA
- Session on privacy by design at Computers, Privacy and Data Protection (CPDP'13) → SIEMENS and CNR
- One-day training course on the ActionGUI technology, discussion of future extensions of ActionGUI and potential commercial impact of the technology. Participation of → IMDEA

Joint PhD supervision
- Joint PhD supervision → IMDEA

ATOS collaborations can be summarised in Table 2.

<table>
<thead>
<tr>
<th></th>
<th>JR</th>
<th>JP</th>
<th>JPP</th>
<th>JOE</th>
<th>JPhD</th>
</tr>
</thead>
<tbody>
<tr>
<td>CNR</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>ETH</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IMDEA</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>INRIA</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>KUL</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>LMU</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SIEMENS</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>SINTEF</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>UDE</td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>UMA</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>UNITN</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 2-ATOS Collaborations

Joint research and publications
- Joint research on model-driven security and ActionGUI → IMDEA
- Submitted paper entitled ‘Secure OCL queries’ → IMDEA
- Submitted journal paper entitled ‘A Model-Driven Methodology for Developing Secure Data-Management Applications’ to Transactions on Software Engineering (TSE) → ATOS, IMDEA
- Joint research on model-based vulnerability testing → SIEMENS
- Joint publication entitled 'VERA: A flexible model-based vulnerability testing tool' → SIEMENS
- Ongoing research on security protocol abstractions → INRIA

The collaborations where ETH is involved can be seen in Table 3.
**Table 3-ETH Collaborations**

<table>
<thead>
<tr>
<th>JR</th>
<th>JP</th>
<th>JPP</th>
<th>JOE</th>
<th>JPhD</th>
</tr>
</thead>
<tbody>
<tr>
<td>CNR</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ATOS</td>
<td>✓✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IMDEA</td>
<td>✓✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>INRIA</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>KUL</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>LMU</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SIEMENS</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SINTEF</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>UDE</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>UMA</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>UNITN</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**IMDEA**

**Joint research and publications**
- Joint research on model-driven security, ActionGUI → ETH
- Submitted paper entitled ‘Secure OCL queries’ → ETH
- Submitted paper to ASIACRYPT’13 → SIEMENS
- Submitted journal paper entitled ‘A Model-Driven Methodology for Developing Secure Data-Management Applications’ to Transactions on Software Engineering (TSE) → ETH, ATOS
- Joint publication entitled 'Automatic Quantification of Cache Side-Channels' at CAV'12 → SIEMENS

**Joint organization of events**
- One-day training course on the ActionGUI technology, discussion of future extensions of ActionGUI and potential commercial impact of the technology. Participation of → ATOS
- Co-organization of QASA’13 workshop, affiliated with ESORICS, September 2013 → CNR

**Joint PhD supervision**
- Joint PhD supervision with → ATOS

The summary of joint activities for IMDEA can be seen in Table 4
**INRIA**

**Joint research and publications**
- Work in Progress on a survey on synthesis mechanism \(\rightarrow\) CNR
- Ongoing research on security protocol abstractions \(\rightarrow\) ETH
- Joint publication entitled 'Towards trust-aware and Self Adaptive systems' \(\rightarrow\) UMA
- Joint publication entitled ‘Verification of ATL Transformations Using Transformation Models and Model Finders’ \(\rightarrow\) ATOS
- Joint publication entitled ‘Checking Model Transformation Refinement’ \(\rightarrow\) ATOS
- On-going joint research to extend previous work on trust-aware and self adaptive systems \(\rightarrow\) UMA

**Joint project proposal**
- Funded project proposal. DIVERSIFY (FET-STREP on call 9), coordinated by INRIA: synthetic software diversity for secure collaborative systems \(\rightarrow\) SINTEF
- Funded project proposal. HEADS (STREP on call 10): software engineering for the future internet continuum \(\rightarrow\) SINTEF (coordinator)

**Joint organization of events**
- IFIP/NESSoS/ANIKETOS/ChoREOS Spring School On 'Trustworthy Services and Systems' \(\rightarrow\) ATOS, CNR, UMA
- FIA pre-workshop on Future Internet Services \(\rightarrow\) CNR, UMA (in cooperation with ANIKETOS and CHOREOS projects)

**Joint PhD supervision**
- Joint PhD supervision \(\rightarrow\) UMA

Joint activities for INRIA are summarized in Table 5.
Joint research and publications

- Submitted paper entitled ‘Risk-based prioritization and selection of change patterns’ → UNITN
- Joint research on distributed access control → UNITN
- Joint research on ‘Evaluating Text Features as Indicators of Software Vulnerabilities’ → UNITN
- Submitted paper at STM’13 → UNITN
- Joint research on Jsand → SIEMENS

Joint organization of events

- Organizing ESSoS’14, in collaboration with → UNITN and SIEMENS

The summary of the joint activities carried out by KUL are summarized in Table 6.
Joint research and publications

- Joint publication on 'A Toolchain for Designing and Testing XACML Policies' → CNR
- Work in Progress on 'UWE - XACML toolchain' → CNR
- On-going research on 'Secure Navigation Paths', technical report in progress → SIEMENS

The collaboration tables for LMU can be seen in Table 7.

<table>
<thead>
<tr>
<th></th>
<th>JR</th>
<th>JP</th>
<th>JPP</th>
<th>JOE</th>
<th>JPhD</th>
</tr>
</thead>
<tbody>
<tr>
<td>ATOS</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CNR</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ETH</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IMDEA</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>INRIA</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>KUL</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SIEMENS</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SINTEF</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>UDE</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>UMA</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>UNITN</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 7 - LMU Collaborations

SIEMENS

Joint research and publications

- Submitted joint paper on applications of trust to web services for the Smart grid scenario → UMA
- Submitted joint paper entitled ‘Receiver-location Privacy in WSN under Eavesdropping and Node Compromise Attacks’ → UMA
- Joint research on model-based vulnerability testing → ETH
- Joint publication entitled 'VERA: A flexible model-based vulnerability testing tool' → ETH
- Joint research on Jsand → KUL
- Submitted paper to ASIACRYPT'13 → IMDEA
- Joint publication entitled 'Automatic Quantification of Cache Side-Channels' at CAV'12 → IMDEA
- On-going research on 'Secure Navigation Paths', technical report in progress → LMU

Joint events organization
• Session on privacy by design at Computers, Privacy and Data Protection (CPDP’13) → CNR and ATOS
• Organizing ESSoS’14, in collaboration with → KUL and UNITN

**Joint PhD supervision**

• Joint PhD supervision → UMA

Table 8 shows the collaborations carried out by SIEMENS.

<table>
<thead>
<tr>
<th></th>
<th>JR</th>
<th>JP</th>
<th>JPP</th>
<th>JOE</th>
<th>JPhD</th>
</tr>
</thead>
<tbody>
<tr>
<td>CNR</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>ETH</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ATOS</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>KUL</td>
<td>✓</td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>IMDEA</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>INRIA</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>LMU</td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SINTEF</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>UDE</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>UMA</td>
<td>✓</td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>UNITN</td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

*Table 8-SIEMENS Collaborations*

**Joint research and publications**

• Development of CORAS extension to support the development of an Information Security Management System (ISMS) → UDE
• Planned joint research on ‘Method for balancing risk and cost in the SDLC’ → UDE
• Joint publication entitled ‘An approach to select cost-effective risk countermeasures’ (DBSec’13) → UNITN
• Joint publication entitled ‘An approach to select cost-effective risk countermeasures exemplified in CORAS’ (Technical Report) → UNITN
• Collaboration in ITEA2 DIAMONDS project → CNR

**Joint project proposal**

• SESAR WP-E Project EMFASE (Empirical Framework for Security Design and Economic Trade-off) → UNITN
• Funded project proposal. DIVERSIFY (FET-STREP on call 9): synthetic software diversity for secure collaborative systems → INRIA (coordinator)
• Funded project proposal. HEADS (STREP on call 10): software engineering for the future internet continuum, coordinated by SINTEF → INRIA
• Proposal for a Norwegian research and innovation project funded by the Research Council of Norway → UMA, UDE (as guest researchers)

**Joint PhD supervision**
The collaborations carried out by SINTEF can be seen in Table 9.

<table>
<thead>
<tr>
<th>Joint PhD supervision</th>
<th>UNITN</th>
</tr>
</thead>
</table>

Table 9-SINTEF Collaborations

**UDE**

**Joint research and publications**

- Joint publication in CD-ARES entitled “Combining Goal-oriented Requirements Engineering Methods” → UNITN
- Joint research on problem frames and trust → UMA
- Planned joint research on ‘Trust-based automatic policies synthesis’ → UMA
- Development of CORAS extension to support the development of an Information Security Management System (ISMS) → SINTEF
- Planned joint research on ‘Method for balancing risk and cost in the SDLC’ → SINTEF
- On-going research on ‘Computer-Aided Requirements Conflict Analysis considering Service Oriented Architectures’ → UNITN
- Joint publication entitled ‘Combining Goal-oriented and Problem-oriented Requirements Engineering Methods’ at CD-ARES 2013 with → UNITN
- Planned joint research to use SI* threat modelling with the attack graph approach → CNR

**Joint project proposal**

- Proposal for a Norwegian research and innovation project funded by the Research Council of Norway → SINTEF where UMA and UDE participate as guest researchers.

**Joint organization of events**

- Organization of the second ESSoS doctoral symposium in Paris on February, 27th 2013 → CNR

Table 10 summarises the joint activities carried out by UDE.
Joint research and publications

- Joint publication on “Detecting Insider Threats: a Trust-Aware Framework” published at conference ARES → UNITN
- Joint publication 'A tool for secure service orchestration' → CNR
- Submitted joint paper on applications of trust to web services for the Smart grid scenario → SIEMENS
- Submitted joint paper entitled ‘Receiver-location Privacy in WSN under Eavesdropping and Node Compromise Attacks’ → SIEMENS
- Joint publication entitled 'Towards trust-aware and Self Adaptive systems' → INRIA
- Joint research on problem frames and trust → UDE
- Planned joint research on ‘Trust-based automatic policies synthesis’ → UDE
- On-going joint research to extend previous work on trust-aware and self adaptive systems → INRIA

Joint project proposal

- Proposal for a Norwegian research and innovation project funded by the Research Council of Norway → SINTEF where UMA and UDE participate as guest researchers.

Joint events organization

- 7th International IFIP WG 11.11 on Trust Management, June 2013 → CNR
- IFIP/NESSoS/ANIKETOS/ChoREOS Spring School On 'Trustworthy Services and Systems' → ATOS, INRIA, CNR
- FIA’13 session in Dublin on 'How far do we have to go to make the Internet secure?' → CNR (together with HP, TSSG). This session was organized in conjunction with projects BIC and Seccord.
- FIA pre-workshop on Future Internet Services → INRIA, CNR (in cooperation with ANIKETOS and CHOREOS projects)

Joint PhD supervision

- Joint PhD supervision → INRIA
- Joint PhD supervision → SIEMENS
Table 11 shows the collaboration activities carried out by UMA.

<table>
<thead>
<tr>
<th></th>
<th>JR</th>
<th>JP</th>
<th>JPP</th>
<th>JOE</th>
<th>JPhD</th>
</tr>
</thead>
<tbody>
<tr>
<td>CNR</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>✓✓ ✓</td>
<td></td>
</tr>
<tr>
<td>ATOS</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>ETH</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>IMDEA</td>
<td>✓</td>
<td>✓</td>
<td>✓✓ ✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>INRIA</td>
<td>✓</td>
<td>✓</td>
<td>✓✓ ✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>KUL</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>LMU</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>UDE</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>SINTEF</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>SIEMENS</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>UNITN</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td></td>
</tr>
</tbody>
</table>

Table 11-UMA Collaborations

**UNITN**

**Joint research and publications**

- Joint publication entitled ‘PERSONA: a personalised data protection framework’ → ATOS, CNR and Technical university of Eindhoven
- Submitted paper entitled ‘Risk-based priorization and selection of change patterns’ → KUL
- Joint research on distributed access control → KUL
- On-going research on ‘Computer-Aided Requirements Conflict Analysis considering Service Oriented Architectures’ → UDE
- Joint publication in CD-ARES entitled ‘Combining Goal-oriented Requirements Engineering Methods’ → UDE
- Joint publication entitled ‘An approach to select cost-effective risk countermeasures’ (DBSec’13) → SINTEF
- Joint publication entitled ‘An approach to select cost-effective risk countermeasures exemplified in CORAS’ (Technical Report) → SINTEF
- Joint publication on “Detecting Insider Threats: a Trust-Aware Framework” published at conference ARES → UMA
- Submitted paper at STM’13 → KUL
- Joint publication entitled ‘Combining Goal-oriented and Problem-oriented Requirements Engineering Methods’ at CD-ARES 2013 → UDE

**Joint project proposal**


**Joint events organization**

- Organizing ESSoS’13, in collaboration with → KUL and SIEMENS
The collaboration activities performed by UNITN are shown in Table 12.

<table>
<thead>
<tr>
<th></th>
<th>JR</th>
<th>JP</th>
<th>JPP</th>
<th>JOE</th>
<th>JPhD</th>
</tr>
</thead>
<tbody>
<tr>
<td>ATOS</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CNR</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ETH</td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>IMDEA</td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>INRIA</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>KUL</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>LMU</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>SINTEF</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>SIEMENS</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>UDE</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>UMA</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

*Table 12-UNITN Collaborations*

By observing the above peer-to-peer tables that describe the collaborations that happened within the NESSoS core partners for Y3, we can notice that all the partners have collaborated with other partners ranging the number of collaborations from two to seven partners in some cases. Figure 1 shows the research collaborations that are taking place within the NESSoS core partners. We can observe that all the partners are collaborating with at least two other partners. In some cases the research that has been carried out has led to joint publications. Figure 2 shows graphically the occurrence of joint publications.

In the analysis that we have performed for the joint activities performed for Y3 we can notice that a difference with respect to the analysis performed last year (see [D4.2_I]) is that some subcategories such as *Joint Project Proposal* and *Joint PhD Supervision* have become relevant on their own and the results on the analysis are shown in Figure 3 and Figure 5 respectively.

During the third year, NESSoS partners have been involved in the organisation of events to a greater extent than in the previous year. This year nine partners have been involved in the organisation of events together with other partners. In some cases the efforts were carried out by three different partners, as it can be seen in Figure 4.
Figure 1 Joint Research
Figure 2 Joint Publications
Figure 4 Joint Organisation of Events
2.2 Collaborations with Associate Partners

Most of the collaborations that were established with associated partners during the second year are still happening for the third year. We remind them here again.

**CNR**

- Paola Inverardi (and her group), University of l'Aquila
  - Definition of an approach for analysis and monitoring of dependability and security in dynamic system connection
- Yves le Traon, University of Luxemburg
  - Methodologies for automating Test Generation based on Access Control Policies specifications.
- Matthias Buechler (Technische Universität München Institute of Informatics, Alexander Pretschner group)
  - Integration of methodologies for Security Testing of Web Applications with approaches based on access control policies

**SIEMENS**

- Joint publications
KUL

- SAP (work inspired by SIEMENS): web security

---

SINTEF

- Alexander Pretschner is guest scientist in the Norwegian part of the DIAMONDS project, which is led by SINTEF

Besides that, NESSoS associated partners participated into several NESSoS activities, in particular, Jan Jürjens and Valerie Issarny (INRIA) were part of the organising committee of ESSoS’13 as Program committee chair and general chair respectively. Associated partners have been invited to attend the NESSoS meetings. There is a description of their involvement in these meetings for the last year in Section 3.1 but we can see that for this year, at least one associate partner have attended each of our meetings.
3 NESSoS Activities for Achieving Integration

The integration of research agendas requires the alignment of activities with other communities working on similar areas, or in some cases in areas where we believe NESSoS research topics can be beneficial to the whole research community.

This section presents a detailed description of the activities that have been carried out by NESSoS partners in order to expand the secure service engineering community. It is organized as follows. Section 3.1 addresses the meetings where NESSoS partners discuss about the evolution of the project. The NeSSoS flagship event, namely the ESSoS conference, is presented in Section 3.2. Then, in Section 3.3, we provide insight into the collaboration activities that have been performed with external communities. Section 3.4 discusses other relevant events where NESSoS, although more passively, has had presence. Section 3.5 describes activities targeting at education and training purposes, whereas Section 3.6 summarizes one of the most important expected outputs from NESSoS: the roadmap, which is fully available in [D4.2_partII].

3.1 NESSoS Meetings

NESSoS meetings are the main tools for partners to come together and discuss about issues related to the project. Our policy for holding these meetings is always to have them co-located with major events, which allows the other communities to learn about NESSoS. As usual, whenever the ESSoS conference is taking place the NESSoS consortium organizes a meeting together with this conference. This year we held our meeting at the INRIA premises in Paris in February 2013. The following meeting was held in Malaga together with the NESSoS/ANIKETOS/CHOREOS Spring school in May 2013, which in turn was held in conjunction with the IFIP Trust Management conference 2013, also in Malaga. The last meeting of the NESSoS consortium during this reporting period took place in Bertinoro from 4th to 6th of September 2013 together with the FOSAD summer school, which is one of the main PhD schools supported by NESSoS.

We have improved NESSoS meetings with workshops that foster the scientific exchange between NESSoS associate and partners. During this reporting period the workshops that have taken place have been the following.

- Meeting in INRIA (Paris), February 2013. The ESSoS Doctoral symposium was this time considered as the NESSoS workshop and was considered as part of the meeting.
- Meeting in Malaga, May 2013. For this meeting we held the workshop on Security and Privacy for Evolvable, Adaptive Mobile Systems. The speakers of this workshop were two of the NESSoS associate partners, Ruth Breu and George Spanoudakis and the NESSoS member from SINTEF, Ketil Stoelen. Ruth Breu presented her work entitled 'From Model-Driven Security to Living Models - Security Engineering for Large IT Infrastructures’. The work presented by George Spanoudakis was entitled ‘Secure Service Composition: A Patterns Based Approach’.
Ketil Stoelen gave an overview of the work done in NESSoS under WP10 on ‘Risk and Evolution’.

- Meeting in Bertinoro, September 2013. One of our associated partners, Sokratis Katsikas attended the NESSoS meeting in Bertinoro. As usual, an important part of the meeting was to hold a workshop on a NESSoS research topic. The topic of the workshop for this edition was ‘Mobile Devices Security and Privacy’. The workshop was devoted to discuss the latest achievements of the participants on the mobile devices security and identify potential collaboration opportunities.

The following key speakers illustrated several scientific results and in particular software tools (as the MADAM and iCareMobile solutions) for improving the mobile devices security.

- Alessandro Armando University of Genova&FBK Trento
- Mauro Conti, University of Padova
- Animesh Pathak, INRIA
- Andrea Saracino, CNR

The meeting was open and attended also by several students of the FOSAD school that was running in parallel in Bertinoro. Several initiatives for cooperation were triggered by the discussions.

3.2 Flagship Event: ESSoS Conference

The International Symposium on Engineering Secure Software and Systems celebrated in 2013 its fifth edition. This conference has been chosen as the NESSoS flagship event as the topics of the symposium clearly considered most of the research topics that are being addressed by the consortium.

The development of secure software and services is a challenging issue that is becoming a core ingredient in today’s systems. The complexity of modern systems and the huge variety of available software technologies makes the consideration of engineering techniques that could improve the security properties of those systems and applications essential. This task, however, is far from being straightforward and would greatly benefit from drawing the attention from academia. Surprisingly, very few conferences are devoted to these issues.

Hence the idea of this symposium, the goal of which is to bring together researchers and industrial parties to advance in the area of secure software engineering. As the interests of the ESSoS community and NESSoS are linked, NESSoS is one of the sponsors of the event and collaborates with its organization, as some NESSoS partners are part of the steering committee. This year’s event was held in Paris (France) in the premises of INRIA and organized by Valerie Issarny. The programme included two days of research papers. Besides the specific programme based on reviewed papers, this year the second edition of the ESSoS Doctoral Symposium was organized by NESSoS (CNR and UDE, more precisely) in order to give PhD students in the area the opportunity to present their work, share opinions and obtain feedback. The programme of the doctoral symposium included a keynote talk by Wouter Joosen (KUL) in which he talked about the PhD perspectives on software engineering and security.
3.2.1 Panel on NESSoS Roadmap

The programme of ESSoS included a panel where the main focus was to present to the audience the NESSoS roadmap. The presentation of the NESSoS roadmap at this venue is very appropriate as we have pointed out the main area of research of the ESSoS conference attendees is shared with NESSoS.

The panel was chaired by Fabio Martinelli (CNR) who gave an overview of the project to the audience. Carmen Fernández (UMA) introduced the NESSoS roadmap to the audience in order to start the discussion. Then the other panellists gave their opinions and views on the topics proposed by NESSoS. The panellists were

- Laurie Williams from North Carolina State University (US). She was one of the invited speakers at ESSoS for the 2013 edition.
- Jan Jürjens from Dortmund University (Germany). He is a NESSoS associate partner.
- Alexander Pretschner from the Technical University of Munich (Germany). He is a NESSoS associate partner.
- Volkmar Lotz, SAP Research (France). He is a member of the NESSoS IAB.
- Wouter Joosen (KUL) as the NESSoS research stream leader.

The discussion focused on the past, present and future of secure software engineering and what research should be conducted to in this area.

- Need for quantitative methods for secure software engineering.
- Service composition.
- Usability.
- Runtime aspects: context and evaluation.
- Validation is very important but in a way that the results are meaningful

From the industry perspective there were some important issues mainly raised by the representative from the NESSoS IAB, Volkmar Lotz from SAP:

- Economics. In particular, what is the return on investment in security.
- Static code analysis is a key factor for discovering vulnerabilities.
- Companies need to be provided with appropriate tools that will make their work easier and more profitable.
- Patches: pragmatic aspects to consider when shutting down systems for applying patches.

3.3 Participation in Activities with Other Communities

Next, we will describe the NESSoS activities carried out together with other communities. These activities usually happened in the framework of major events where we considered NESSoS could enrich the proposed agendas by including its view on secure service engineering. The major events where these activities took place for the last reporting period were the following:

- Annual Privacy Forum
- Computers, Privacy and Data Protection conference
- Future Internet Assembly week.
- IFIP community
• BIC project meetings
• Cyber Security and Privacy (CSP) forum
• Schloss Dagstuhl venue
• ESORICS and its collocated workshops

Subsequent subsections give insight into the activities performed within the scope of each of the aforementioned events.

3.3.1 Annual Privacy Forum and the Second NESSoS Industry Seminar

The Annual Privacy Forum (APF) 2012 was held in Limassol, Cyprus from the 10th to the 11th of October 2012. The Forum is based on the idea that privacy is a fundamental need and does not have to be threatened by electronic communications. Therefore, this event provides a forum to the major stakeholders in the field in order to close the loop from research to policy. The APF 2012 was organized by the European Commission Directorate General for Communications Networks, Content and Technology (DG CONNECT), the European Network and Information Security Agency (ENISA) and the Department of Computer Science of the University of Cyprus and is an official event of the Cypriot EU-Presidency.

NESSoS participated in the APF 2012 as one of the four partners of the event. Moreover, NESSoS organized the second NESSoS industry seminar entitled “Privacy By Design and Secure Software Engineering”. The chair of the workshop was Aljosa Pasic from Atos, chair of the NESSoS advisory board.

The workshop addressed the problem of building security in the design process. The engineering of secure software services from the very beginning in system analysis and design can contribute to reduce the amount of system and service vulnerabilities and enable the systematic treatment of security needs. The workshop analyzed the interaction of privacy by design and secure software and service engineering. Moreover, the workshop took into account the challenges derived from the emergence of Future Internet services and applications, such as the heterogeneity of security and privacy characteristics amongst services from different organizations and providers, fragmentation of ownership of both services and content and the complexity of implicit and explicit relations among the participants.

Aljosa Pasic introduced NESSoS and discussed on the potential application of a model-driven design approach to enhance user's privacy in the software development lifecycle as it has been done to boost security. Then, the following talks where provided during the workshop:

1. The need to standardize location privacy protection policies – A look at the IETF.
   Speaker: Jorge Cuellar, Siemens
2. Principles of Privacy by Design in Smartmetering: issues of importance to privacy engineers and technologies.
   Speaker: Claire Vishik, Intel
3. Use of USDL-SEC for privacy goals.
   Speaker: Francesco Di Cerbo, SAP
   Speaker: Nick Wainwright, HP Labs.
Integration with NESSoS. Privacy is a hot topic in the research agenda for Europe. This includes the industry stakeholders. For this reason it seemed a good venue for the NESSoS consortium to hold their second industry seminar and take advantage of the event in order to increase the number of participants. Thus, as we considered that Privacy by design is a very important issue to be discussed with the industry stakeholders we believed that the APF was the perfect venue for holding this event.

3.3.2 Computers, Privacy and Data Protection Conference

The CPDP Conference on Engineering Privacy-aware Systems and Services was held in Brussels (Belgium) from the 23rd to the 25th of January 2013. The purpose of this conference was to bring together all the interested practitioners in the area of privacy. The conference welcomed 650 guests providing a platform for privacy stakeholders, which included academia, public and private sectors and civil society. Both the Council of Europe and the Polish Permanent Representation to the European Union provided their collaboration. Within this context, NESSoS organized a panel on ‘Engineering Privacy-aware Systems and Services’. D. Le Metayer, from INRIA, moderated this panel together with Fabio Martinelli, from CNR. They presented an overview of the project and its main objectives concerning privacy. Then, two members of the project gave more details about the work on privacy carried out within the project. Jorge Cuellar from Siemens presented the privacy problems that will arise in Future Internet scenarios due to the use of devices such as RFID or sensors. In this sense Ruben Rios, from UMA, discussed the work that has been done concerning location-privacy for Wireless Sensor Networks and their applications to some NESSoS scenarios such as smart grid. The session included a wrap-up and summary considering also the audience comments and suggestions.

Integration with NESSoS. Again, privacy was the key issue of the CPDP conference. Therefore, NESSoS organized a panel on engineering privacy aware systems that reached a broader audience than the one in the APF.

3.3.3 Activities organized during the FIA Week in Dublin

The Future Internet Assembly week was held in Dublin (Ireland) from the 8th to the 10th of May 2013 in association with the Irish presidency of the Council of the EU. FIA is a research community driven initiative supported by more than 150 research projects that have recognised the need to strengthen European activities on the Future Internet (FI) to maintain European competitiveness in the global marketplace. The theme of this year’s edition was ‘Future Internet accelerates innovation’. As usual, besides the Open Plenary Day the FIA programme included two days working sessions that included 12 of them. These sessions were selected by the FIA Steering Committee from a considerable number of submissions.

Integration with NESSoS. As in previous editions of FIA NESSoS was present in this event as the main application scenario of NESSoS is the FI. Thus, NESSoS co-organized a session and also participated in a pre-FIA workshop together with other projects.

3.3.3.1 Session at FIA

NESSoS submitted a proposal for a session together with the EU projects BIC and SECCORD, which was finally accepted and held on the 10th of May 2013 in Dublin. The title
of the session was “How far do we have to go to make the Internet Secure?” The organisers of the sessions were Fabio Martinelli and Carmen Fernandez from NESSoS, Nick Wainwright and Paul Malone from SECCORD and Jim Clarke from BIC.

The session provided a forward looking view on relevant trustworthy ICT future issues and how security-by-design can address these, looking at these issues both at a European and international level. Each actor in the infrastructure, data and services space must play their part in making the ecosystem secure. With this in mind, we identified priority areas that were addressed in three distinct sessions. We invited two speakers from each of the sessions who are well known in the respective areas of expertise, including representative for academia, industry and SME. Thus, we covered most of the topics that are supposed to influence the design of security in FI services. The structure of the session was as follows:

1. **Secure network and infrastructures** – where are the new vulnerabilities and how to address them?
   - Chair: Brian Honan, IRISS.
   - Participant: Dirk Kuhlman, HP Labs.
   - Participant: Ruben Rios, University of Malaga.
2. **Security and big data** – what are the issues and how can we respond?
   - Chair: Nick Wainwright, HP Labs.
   - Participant: Stephen O’Boyle, Espion.
3. **Trustworthy software and services** – how far can we go beyond the current state of the art?
   - Chair: Rodrigo Diaz, Atos.
   - Participant: Hisain Elshaafi, TSSG, Waterford Institute of Technology.
   - Participant: Mike Surridge, University of Southampton

### 3.3.3.2 Pre-FIA Workshops

The CHOREOS project proposed a workshop with the title ‘Sustaining Service-Oriented Computing in the Future Internet’. Even though, the CHOREOS project was the proponent of the workshop they asked for contributions to other projects such as FI-WARE, CONNECT, NESSoS and ANIKETOS. Thus, the participants from the NESSoS project to this workshop were INRIA, CNR and UMA. All of the projects showed their views and goals and shared experiences and common points of research among them.

### 3.3.4 IFIP Community

The International Federation for Information Processing is an international organization in Information and Communication Technologies and Sciences. This organization represents IT societies from countries covering the five continents. IFIP is composed by different technical committees (TC), which are also composed by different Working Groups (WG). IFIP TC 11 is the technical committee on Security and Privacy Protection in Information Processing Systems. Being security the main area of research of this TC it seems reasonable that NESSoS approaches some of its WG in order to organize joint events.
Integration with NESSoS. IFIP is an international organisation covering most of the areas on Information technology, including security. For this reason, some efforts from NESSoS were driven towards the integration with this community. Thus, we have participated in events organised by some of its WGs and have joined them by fostering a new WG aligned with the NESSoS research.

3.3.4.1 IFIP Conference on Trust Management

Thus, NESSoS was involved in the organisation of the IFIP WG 11.11 conference on Trust Management. This conference was held in Malaga (Spain) in June 2013. It was organized by the NESSoS partners Fabio Martinelli (CNR) and Carmen Fernandez and Javier Lopez (UMA). The event had two invited talks. The first invited talk was delivered by Pierangela Samarati, who is one of the NESSoS NALaB members. The title of her talk was ‘Data security and privacy in the cloud’. The second invited talk was given by Jorge Cuellar (SIEMENS). The title of his talk was ‘Security: proactive or reactive? Science or best practices?’

Besides these two very NESSoS related invited talks the program of the conference included the third NESSoS industry seminar. The title of this edition of the seminar was ‘Security by Design: from Theory to Practice’. The seminar was split into three different slots. The first slot was an invited talk delivered by Amardeo Sarma from NEC Labs. Then, the slot entitled ‘Lessons from Industry In Secure Software and Service Engineering’ included the following talks:

- ‘Reducing Cost by Assurance in the Early Phases of SDLC’ by Pawel Krawtzyk (AON)
- ‘Markets for Discovery of Software Vulnerabilities or the New Malware’ by Alfonso De Gregorio (BeeWise)
- ‘Lessons from ANIKETOS Project’, Dhouha Ayed (Thales)

There was also a slot on ‘Security by Design and E2E Trust’ that included the following talks:

- ‘Software Assurance and Cybersecurity’ by Volkmar Lotz (SAP)
- ‘Identity Assurance’ by Paul Thomas (Microsoft)

The Industry seminar ended with a demo session on the ANIKETOS project presented by Erkuden Rios (Tecnalia).

More information about the Industry seminar can be found in [D14.5].

3.3.4.2 Creation of the IFIP WG 11.14 on Secure Engineering

NESSoS consortium believes that it is essential for the success of the project to continue the work done by it. This could be achieved by creating a Working Group in the area of secure engineering. Thus, we submitted a proposal to IFIP for a new WG under their auspices, which was successful.

The WG will leverage on the experience and community developed by NESSoS. This new WG aims to provide a forum for cross-disciplinary investigation of “secure engineering” with attention also at the software-services and system aspects. The working group will bring together researchers with an interest in several area of computer science, including, security,
security engineering, service engineering, software engineering, formal methods and related fields.

The main goals of the WG will be aligned with many of the goals of NESSoS and are listed below:

- The creation of a long lasting research community on engineering secure services and software systems.
- Maintaining a research roadmap in the area of secure service engineering.
- Maintaining a workbench for secure service engineering tools.
- Contribution to education, training, dissemination.
- Reduction of gap between industry and research best practices.

The proponents of the WG and the members of the Executive Board of the WG are the following:

Chair: Fabio Martinelli (CNR)
Vice-chairs: Wouter Joosen (KU Leuven), Fabio Massacci (University of Trento)
Secretary: Javier Lopez (University of Malaga)
Liaison with Industry: Aljosa Pasic (ATOS), Jorge Cuellar (Siemens)

### 3.3.5 BIC Project Meetings

The Building International Cooperation (BIC) for Trustworthy ICT is a EU-funded project coordinated action that intends to promote research programmes in the area of Trustworthy ICT with new emergent countries such as Brazil, India and South Africa. In order to achieve their goals, the project organizes different events for bringing together researchers of all the aforementioned countries and European researchers. One of these events is the BIC Annual Forum. As a first step of the realization of this forum, topics of interests in the area of trust and security were identified to be included in the agenda.

**Integration with NESSoS.** In its effort of integrating research agendas NESSoS attended several BIC meetings in order to learn how the integration can be done outside Europe. Several topics of interest to NESSoS partners were discussed in these meetings. Privacy and, especially, trust, were widely covered as context-dependent areas, where location and other factors determine the way they must be ensured. In order to make security easily accessible by different users’ profiles, security management was identified a crucial issue to address. Also, assurance and risk and cost-awareness along the SDLC were considered primary areas of research that need further insight.

BIC held one of its workshops together with the IFIPTM conference, which was sponsored by NESSoS. This event was held in Malaga (Spain), 5-6 of June 2013 and was also co-organised by the DIMACS project supported by the National Science Foundation (NSF) in the US. The topic of the event this year was on Trustworthiness, Accountability and Forensics in the Cloud.

As me mentioned in Section 3.3.3.1 BIC was one of the co-organisers of the FIA session together with NESSoS.
3.3.6 Cyber Security & Privacy EU Forum (CSP)

NESSoS has participated in several tracks of CSP Forum\(^1\), including the opening session, as well as a session, co-organised by NESSoS, on standardization and cloud assurance. ATOS represented NESSoS in this event. Finally, Atos also represented NESSoS at the Networking and Coordination cluster of CSAs in Trust and Security and participated in all discussions on future clustering and NIS (Network and Information Security) platform. The NIS platform is a new initiative that aims at being a platform for bringing together policy and technical experts to debate on the current and future challenges of cyber security. The platform is split into three different WG being security one of them. It is chaired by Fabio Martinelli and other NESSoS partners are members of this WG.

NESSoS also participated in a joint session on ‘Assurance in the cloud’ together with Cumulus and Assert4SOA. The coordinator of this session was Ernesto Damiani.

3.3.7 Schloss Dagstuhl

The schloss Dagstuhl-Leibniz Center for Informatics is one of the most popular venues for computer scientists to meet. It fosters the exchange of knowledge among practitioners, young researchers and very well known senior researchers.

There are several bodies and boards for the activities of these events. One of these boards is the Industrial Curatory Board. SIEMENS, and more specifically, Jorge Cuellar, is part of it. As part of the board, he attended the meetings they organized.

NESSoS partners have been directly involved in the organization of some seminars at Dagstuhl and others have attended them.

- Boris Köpf from IMDEA co-organized the seminar on Quantitative Security Analysis. He also delivered a talk on "Automatic Quantification of Cache Side Channels". This seminar took place from 25\(^{th}\) to 30\(^{th}\) of November 2012. Fabio Martinelli was a speaker for this seminar.
- Maritta Heissel from UDE co-organized the seminar on Engineering Resilient Systems: Models, Methods and Tools
- Carolina Dania participated on the seminar Automated Reasoning on Conceptual Schemas by presenting the talk on OCL2FOL: Using SMT solvers to automatically reason on conceptual schemas with OCL constraints about the work performed by IMDEA

Integration with NESSoS. The events and seminars organized at Dagstuhl are very-well known by their excellence and quality. As it was shown in [D4.2 partI] this is a key community to approach by NESSoS. In particular, the seminar on Quantitative Security Analysis, co-organized by Boris Köpf (IMDEA) dealt with one of the emerging topics considered within the NESSoS community, as it can be seen in the roadmap. The emergence of this topic as relevant area of research is also shown by the creation last year, and continuation this year of QASA workshop (see Section 3.3.8).

\(^1\) http://www.cspforum.eu/2013
3.3.8 International Workshop on Quantitative Aspects in Security Assurance (QASA)

The International Workshop on Quantitative Aspects in Security Assurance served as a vehicle to bring together researchers in the area of security assurance and the NESSoS consortium. This event started in 2012 as a co-located event of ESORICS and this year has happened in the same way, together with ESORICS, which is sponsored by NESSoS. Thus, the event took place in the premises of Royal Holloway University (UK) in September 2013. As it happened in the previous edition the organisers were mainly NESSoS partners. Thus, the event was organised by Fabio Martinelli (CNR) and Boris Köpf (IMDEA). Besides the programme composed by the selected papers by the programme committee a panel on ‘Risk Management for IT Security’.

Integration with NESSoS. In this case the integration with NESSoS is very clear as this is an event that has been the result from NESSoS proposed topics of research and it has been organised by NESSoS.

3.3.9 Analysis of the Performed Activities and its Relevance to the NESSoS Community

The goal of this section is to analyse the activities performed under the lens of its relevance to the NESSoS community during the last year. Research areas of interest for NESSoS are first identified and then we identify the research areas covered by the aforementioned activities and check whether they are aligned with NESSoS research areas. The topics of interest of NESSoS are shown in Figure 7 (which are those proposed in the NESSoS roadmap [D4.3_II]).

Figure 6 depicts a bar diagram that makes explicit broader topics covered by the activities described in the previous sections. If we observe the figure we can see that in the area of privacy our participation has been higher. This can be explained by the fact that during the last year the focus of some relevant events such as Annual Privacy Forum, CPDP or CSP has been privacy. We can also observe that our presence in events dealing with the rest of the topics is rather uniform, which shows that we are organising events with a broader range of topics related to NESSoS. If we compare this figure with the figure showing the quantification of the events organised last year we can observe that new topics have appeared such as Requirements engineering, Autonomic Security or Users-Centric Security.

From this analysis we also infer that there are some topics that are not covered by the organisation of events such as Compliance and Run-time Verification and Enforcement. For the case of compliance it is very difficult to spot an event focusing only on it, as it is a very transversal topics that has likely been considered in most of the events we described above. As for Run-time Verification and Enforcement the number of publications show that NESSoS partners are very active in this area although there is not a specific event organised where this topic is relevant.
3.4 Other Events

In this section we are going to report on the events that we did not organise or participate in directly, but we have attended as part of the audience. These events allowed us to find out more about the research trends in the corresponding areas as well to identify those of interest where we can contribute to by having a more active participation.

3.4.1 IEEE Computer Security Foundations Symposium

As stated in [D4.2_I] this conference is an outstanding forum for researchers interested in security, in particular, in formal methods. The last edition was held in New Orleans, Louisiana (USA) from 26th to 28th of June 2013. One of the main influences of NESSoS within this symposium was a panel on the “Emergence Science of Security” where David Basin (ETH) was one of the panellists.

3.4.2 Principles of Security and Trust (POST)

As we mentioned in [D4.2_I] POST is a new conference, which is the result of the merging of several workshop on the area of security and formal methods. Several members of NESSoS (CNR, IMDEA and ETH) are part of the steering committee. In particular, David Basin was 2013’s edition Program Chair. This last edition was held in Rome (Italy) from 16th to 24th of March 2013.

As in previous editions the program included several papers on assurance, and more specifically on verification techniques for security protocols.
3.5 Education and Training Activities

- **e-RISE event 2013**

The eRISE 2013 challenge has been conducted to empirically evaluate security engineering and risk analysis methods. The event has been carried out in May and June 2013. The first part of the experiment took place at the University of Trento, Italy (13-17 May, 2013) and the second one at Dauphine University, Paris, France (13-14 June, 2013). Fifty-seven participants were involved. Five research groups have been invited to join the challenge and to give a tutorial to the participants about their methods on security requirements elicitation and risk analysis. The methods were CORAS from SINTEF, SREP from University of Castilla-la Mancha, LINDUNN from Katholieke Universiteit Leuven, and MPRA from Katholieke Universiteit Leuven. Moreover, two industrial partners have participated by providing two case studies:
  - Siemens with the Smart Metering scenario.
  - National Grid in the UK proposed the Electricity Transmission Network scenario.

- **FOSAD summer school**

The 13th edition of the summer school on Foundations of Security Analysis and Design (FOSAD13, University Residential Centre of Bertinoro, 2-6 September 2013) consisted of seven main courses given by experts in the field, a tool session dedicated to the presentation of five software tools and related demos, and three open sessions including nine talks given by participants. The number of attendees of this year’s event was 45. NESSoS is one of the organisers of the school together with the project CryptoForma. The commitment of NESSoS with this school is shown in the fact that many members of the FOSAD Steering Committee and some of the speakers of the school were NESSoS partners.

- **Joint ANIKETOS/NESSoS/CHOReOS/IFIP/TM summer school**

NESSoS, in collaboration with the projects ANIKETOS and ChoREOS, and The IFIP WG 11.11 on Trust Management organized the "Spring Ph.D. School on Trustworthy & Secure Service Composition" held from the 27th to the 31st of May 2013 in Malaga, Spain as co-located event of the IFIP/TM conference held the week after. The goal of the school was to provide a forum for researchers and practitioners interested in the latest research developments in the broad area of “trusted and secure composite Future Internet services”. The program of the school included speakers from the three different projects as well as speakers from the WG on Trust Management.

3.6 Roadmapping Activities

The delivery of a roadmap in the area of secure service engineering has been one of the key achievements of the NESSoS consortium in order to integrate research agendas. The roadmap is set up in the basis of the 2020 view for the Future Internet where ICT will evolve towards a more service oriented ICT and there will be a closer tie between the physical and the virtual world.
In this scenario, the NESSoS roadmap has the potential to provide the guidelines for research in the area of secure service engineering for the coming years. The document identifies the research topics that the NESSoS community considers are relevant to be taken into account in the future. The final version of the NESSoS roadmap (see [D4.3_II]) contains an update of the previous versions from previous years ([D4.2_II]) where the topics and actions have been classified into two main categories. On one hand we consider transversal topics to the SDLC and on the other hand enabling methodologies and technologies to ensure trustworthiness at every stage of the SDLC.

The transversal topics include assurance and risk and cost awareness during the SDLC. This means that our proposal is to consider these two topics at every stage of the SDLC in order to ensure that trust and security properties are being held in every phase, and to ensure also that risk and cost are maintained in a controlled way.

Enabling technologies and methodologies include those research areas involved in every phase of the software development lifecycle, ranging from security requirements engineering to runtime verification and enforcement. Given the aforementioned vision of a service-based ICT, a hot topic that has been included in the research agenda is service composition and adaptation. There are other methodologies that should be considered such as user-centric security or, as new topic added as the result of the interest on it from the research community, we consider that the quantitative aspects of security should be taken into account.

On the top of the research topics that we have considered there are certain security properties that should always be ensured such as compliance, trust, identity management or privacy. The topics of the roadmap are depicted in Figure 7.

![Figure 7 Roadmap Topics](image-url)
The inner part of the picture includes the two transversal or cross research topics. The closest layer to the core of the figure corresponds to the enabling technologies, which are tightly related to the SDLC, whereas in the following layer we located those technologies, which are motivated by the increasing complexity of ICT. The properties, which should always be ensures are located in the outer layer of the figure.

A complete description of the roadmap can be found in a separate document [D4.3_II].
4 Report on the NaLAB Activities

As described in the NESSoS DoW, the Network and Liaison Advisory Board (NaLAB) consists of a set of experienced researchers that play a significant role in the scientific community. The main objective for the constituency of this lab is to act as a bridge with international research communities for fostering cooperation with other communities. In order to achieve this objective we invited for this task two very well-known researchers in the different pillar areas of NESSoS, mainly from outside Europe.

The chair of the NaLAB is Javier Lopez from UMA. The members of the NESSoS NaLAB are Ron van der Meyden, Moti Yung, Martin Abadi and Pierangela Samarati.

As part of their involvement in NESSoS we believe that making them participate in the design of the NESSoS roadmap will be very beneficial, as they will bring to it their experience and a broader view from their work and the communities where they work. Thus, we distributed the second version of the roadmap to them and asked for feedback. Their comments and suggestions have been very valuable to us and they are the main update of the version of the roadmap delivered for this year.

Whenever it is possible we try to involve the members of the NaLAB in our activities. Pierangela Samarati was the invited speaker of the IFIPTM conference (see Section 3.3.4).
5 Conclusion

This deliverable shows the activities that the NESSoS consortium has performed during the third year of the project in order to achieve integration of agendas. The analysis performed on these activities has been twofold. On the one hand, we have considered the activities that have been carried out within the consortium. These activities include joint research, joint publications, joint project proposals and joint organisation of events. On the other hand, we have considered those activities that have been done together with other initiatives. In these cases we have analysed the relationship of the activity with NESSoS. After performing this analysis we were able to evaluate the involvement of NESSoS in relation with the research topics that have been considered relevant by the project. In this sense, we could observe that NESSoS has been involved in activities related to most of the NESSoS research topics.

In the future, we will create an evaluation plan to assess the performance and the impact of the activities performed by NESSoS in the research community.
References

[D4.2_I] Engineering Secure Future Internet Services: A Research Manifesto and Agenda from the NESSoS Community. An Updated Version
[D4.3_II] Engineering Secure Future Internet Services: A Research Manifesto and Agenda from the NESSoS Community. An Updated Version
[D12.5] Annual Upgrades of the Dissemination and Communication Deliverable