Network of Excellence

Deliverable D14.3

Report on First industry/research seminar, and on ongoing standardization
Abstract

In the framework of NESSoS project, we are planning to organize a series of workshops on secure software engineering focused on this interplay between industry and academy. In this document we report on the First NESSoS industry seminar, which was collocated with ServiceWave 2011, and was organized with the purpose to introduce the project to the industrial community, and also to collect and analyze industry best practices, current needs and upcoming challenges. Prior to this industry part, scientific community representatives from NESSoS introduced project and state of the art.

This workshop was intended to allow a more structured interaction between industrial and scientific stakeholders in the field of engineering of secure software and services. Last but not least, this workshop was aimed to support the spreading of the academic research excellence in software engineering to the industrial stakeholders thus contributing to increase the trustworthiness of the Future Internet core platform and services.

Various workshop’s participants recommended NESSoS to take actions towards further aligning it with industrial interests so project’s outputs reach its optimum impact in the industrial practices.
Keyword list:

## Document History

<table>
<thead>
<tr>
<th>Version</th>
<th>Type of change</th>
<th>Author(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>Draft Version</td>
<td>Aljosa Pasic (ATOS)</td>
</tr>
<tr>
<td>2.0</td>
<td>Approved by internal reviewers</td>
<td>Aljosa Pasic (ATOS)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Marina Egea (ATOS)</td>
</tr>
</tbody>
</table>
Table of Contents

ABSTRACT .......................................................................................................................... 1

KEYWORD LIST: ................................................................................................................. 2

INDUSTRIAL PRACTICES. ACADEMIC RESEARCH. POSSIBLE SYNERGIES. ................................................................. 2

1 INTRODUCTION .................................................................................................................... 5

2. REPORT ON THE FIRST INDUSTRY RESEARCH SEMINAR ............ 6
   2.1 Opening presentations ................................................................................................. 6
   2.2 Keynote Speech: BSIMM as an Example of Industry Initiative in Software Security ................................................................. 8
   2.3 Industrial Presentations .............................................................................................. 11
   2.4 Panel ......................................................................................................................... 15
   2.5 Conclusions .................................................................................................................. 19

3. ONGOING STANDARDIZATION .................................................................................... 19

4. REFERENCES .................................................................................................................... 22

ANNEX A: TERMS OF REFERENCE FIRST INDUSTRY SEMINAR .......... 23
1 Introduction

NESSoS industry seminars are organized yearly with the intention to raise the awareness in the community Engineering Secure Future Internet Software Services and Systems technologies about the research activities carried out within NESSoS, as well as their progress and results.

The first of these seminars was organized on October 28th in Poznan, in the form of workshop collocated with the 4th ServiceWave conference and in the same week that few other industrial and research events found place in the same setting (e.g. Future Internet Assembly).

The event was organized around 4 main blocks: opening dedicated to the workshop objectives and introduction to the project, keynote speech focused on community building, three industry presentations focused on best practices and the panel focused on better interaction between European industrial and research stakeholders.

This document follows the structure of presentations and describes the most interesting challenges or topics. However, the report is interlacing speakers industry statements with the observation on how does this challenge or topic apply to NESSoS, whether it has already been contemplated or it appears as a new issue.

More details, terms of reference and agenda can be found in Annex A.
2. Report on the First Industry Research Seminar

2.1 Opening presentations

Aljosa Pasic (Atos) is the chairman of NESSoS Industrial Advisory Board (IAB) opened the workshop with the overview of agenda that suffered minor changes and a positioning of secure service engineering. While web applications have been number 1 target of hackers for a while, it is the shift towards software based services that might make things much worse if security is not treated during the early development phases.

The move towards services, that in the presentation was exemplified with “change address” service, increases the emphasis on relationships, negotiations, and agreements. This brings particular challenges for the area of service security. In order to define which security actions and measures will be both required and beneficial for the evolving, reusable or context-aware services, a coherent framework for secure service engineering has to be prepared.

There are a number of different factors and resultant consequences that industry faces, starting with the ever growing problem of lack of expertise. New staff usually does not fit this need for software engineers with “security mind” or security experts with software development skills. Security is difficult to capture with standard software design techniques and is partly a human and social problem and not just a technical one. There is no homogeneous way to represent security concerns and security mechanisms at different levels of software description. Thus, it is difficult for organizations to trace security issues along the phases of software development.

A joint definition and scoping of a new community is an important objective of these NESSoS industry seminars. Service Security and Secure Service Engineering (SSE) covers tools, methods, processes and procedures that will allow practitioners to design, implement, test, deploy, configure, maintain, adapt, use and audit secure and dependable service-based information systems. One of the challenges NESSoS faces is incorporation of existing but scattered know-how, patterns and best practices and their shaping into a single, unified, independent process that industry can use along the whole software development life cycle.

Presentation outlined several problems related to software based services that should also be reviewed by industry seminar and NESSoS project in general in order to prioritize issues:

1. **Requirements:** how to decompose and validate high level concepts (compliance, privacy, trust, risk...) and link them to security requirements?
2. **Complexity:** how to cover all possible mappings between devices/services/stakeholders/data (location, identity…)/context…?
3. **Scale:** how to reason about millions of events in (near) real time (streamreasoning)?
4. **Dynamicity:** how to model it (e.g. dynamic prioritization according to dynamic risk perception)?
5. **Distribution:** how to correlate events from different sources/channels (address new threats)?

Further challenges include adaptable services (so that when regulations, rules, availability or trust changes, a security configuration can adapt automatically), composable (e.g. to derive end-to-end security properties as the result of the overall process linked to the security of individual components), measurable services (e.g. in order to be negotiable between partners as different levels of security and dependability can be traded for costs and/or functionality), etc.

Another objective for this series of events is tune “selling argument”. Although this is almost exclusively industrial terrain, it would be interesting to hear opinion from academic about several possible directions. One approach is consultancy-led and uses the “momentum” when many organizations have to transform and perform migration of their legacy applications to software-based services. It is the right moment to sell “secure by design” argument and align ICT migration with business transformation. Another point of view comes from organizations that are active in managed security services and could provide relevant expertise “on-demand” (e.g. assurance or specialized security services).

Trust and assurance rely on the developments of methods for formal verification of the security engineering methodologies and constructs. Recent development in design methodologies should be taken into consideration as security and dependability oriented processes should not overload software development processes or limit their further development. Suitable processes should therefore employ methods that will allow automated production of high and low level designs and implementation with support for automated production of tests and monitoring. SSE should also support seamless integration with other business processes and management practices. Therefore it should be possible to measure requirements and deliverables using indicators compatible with widely adopted business indicators. Engagement in business decisions and governance will increase strategic alignment of business processes with SSE practices and ensure proper trade-off between security inclusion costs, benefits and security related consequences.

Finally, the results of the survey done among members of NESSoS IAB was briefly presented. After comparison with some other surveys such as Forrester or BSIMM, several common questions or doubts were identified and will be further treated through industry interviews or feedback coming from this event:

- Is SSE a tactical concern or a strategic initiative?
- Are the main incentives for doing SSE linked to risk appetite, culture or assurance profiles?
- Is it clear who is taking risk in cross-organizational service-based applications?
Fabio Martinelli (CNR) the NESSoS project coordinator gave a brief project presentation.

The main project achievement so far has been presented, including infrastructure for the operation of the Joint Virtual Research Lab. This constitutes the main infrastructure for working and is the backbone of the NoE activities. Work has been doing to evaluate security engineering methods and identify relationships among them. NESSoS partners work together to integrate these methods in a sensible way to be used appropriately, thus creating a portfolio for their use. A common body of knowledge (CBK) is another achievement that consists both of research findings and industrial best practices that must be agreed upon, assessed, disseminated and maintained and that can be used to identify possible synergies among partners. In order to support the creation of the long lasting research community on secure software services and systems, several other actions have been presented. In addition, assurance in the Future Internet has been mentioned since the security requirements of Future Internet applications will differ considerably from those of traditional applications. The reason is that Future Internet applications will not only be distributed geographically, as are traditional applications, but they will also involve multiple autonomous stakeholders, and may involve an array of physical devices such as smart cards, phones, RFID sensors and so on that are perpetually connected and transmit a variety of information.

2.2 Keynote Speech: BSIMM as an Example of Industry Initiative in Software Security

Gary McGraw (CIGITAL/BSIMM) opened his presentation with a reflection on the role of software security through the last decade. Security has been regarded as secondary aspects in system design and development. It was often treated as an afterthought and, in many cases; it was taken for granted that security would be provided by external infrastructures. Therefore, ad hoc security and dependability solutions were developed to suit the specific needs of specific systems. Software security, he concluded, is more than just a set of security functions. The security requirements of the entire system may not all be satisfied by eliminating single, isolated weaknesses in the system. Furthermore, their fulfillment cannot be confirmed since the requirements have not been clearly specified in the first place.

He resumed explaining differences between bugs and flaws with illustrative examples and mentioned that, in practice, when it comes to application level vulnerabilities we can find 50% of each. The security mechanisms introduced sometimes by networking people are not directly linked to the specific security requirements of the application. Linking between security mechanisms and requirements is particularly important in case of failures of security mechanisms, when the effects of attacks on the overall security of a system must be determined.

The largest part of presentation focused on BSIMM [1]. The BSIMM is a study of software security initiatives in industry built entirely from observations.
(BSIMM1 was observing 9 initiatives while the last version BSIMM3 observed 42 initiatives). The BSIMM is descriptive and not prescriptive: it does not tell you what you should do; instead, it tells you what everyone else is actually doing. Gary explained that the BSIMM describes the work of 786 software security group (SSG) members working with a satellite of 1750 people to secure the software developed by 185,316 developers. On average, the participants have practiced software security for five years and six months (with the newest initiative being eleven months old and the oldest initiative being sixteen years old in September 2011). When it comes to SSG their role seems very important: they bridge gap between software developments and IT security (mainly network experts) and they are usually recruited among software developers (that receive training in security, rather than the other way round). In average survey shows that there are 2 SSG members or secure software experts for every 100 developers. Almost every organisation has its own SDLC. Many organizations begin with a published methodology such as OWASP CLASP, Microsoft SDL, or the Cigital Touchpoints and then tailor the methodology to their needs. An SSDL process evolves as the organization matures and as the security landscape changes.

BSIMM is based on observation of 109 activities that are placed in 12 practices divided into 4 domains and properly organized through Software Security Framework (SSF). If we compare BSIMM with NESSoS survey done in WP14 we find that NESSoS survey chapter on software development policies would approximately correspond to BSIMM deployment domain with software environment area questions such as on OS and platform patching, Web application firewalls, installation and configuration documentation, application monitoring, change management, code signing.

The software security process will eventually involve release gates at one or more points in the software development lifecycle (SDLC). For example, the SSG can collect security testing results for each project prior to release, but stop short of passing judgment on what constitutes sufficient testing or acceptable test results. This is something similar to what we have observed in NESSoS survey response on feasibility.

Gary did drill down into “architecture analysis” with presentation of activity. It deals with design review for high-risk applications. The organization learns about the benefits of architecture analysis by seeing real results for a few high-risk, high-profile applications. If the SSG is not yet equipped to perform an in-depth architecture analysis, it uses consultants to do this work. Ad hoc review paradigms that rely heavily on expertise may be used here, though in the long run they do not scale. We can also find NESSoS relation and equivalence between domain of BSIMM observation on SSDL touch points and the practise of architecture analysis with NESSoS industrial best practise survey. Activities such as capturing software architecture diagrams, applying lists of risks and threats, adopting a process for review, building an assessment and remediation plan have also been observed in NESSoS survey (see deliverable D 14.2) questions dealing with attackers and patterns, for example. In addition, question 11 from NESSoS survey, for example, corresponds to level 1 activity of security features and design of BSIMM. NESSoS survey observed how European
organisations deal with security problem analysis, security design and security architecture which roughly corresponds to similar observation in BSIMM domain intelligence and practises of security features and design. In addition, NESSoS survey questions 13 tackled code review and comes to the same conclusion like BSIMM observations in the domain SSDL TOUCHPOINTS. Where NESSoS survey differs was for example the use of black box security tools in quality assurance (QA), risk driven white box testing, application of the attack model, code coverage analysis and these might be ideas for the enhancement of NESSoS survey in the future. However, the most important conclusion is the observed need to engage software developers with IT security and architecture discussion. One way to keep security from falling out of the discussion is to have an SSG member attend regular architecture meetings. Another recommendation from BSIMM to NESSoS is related on how to engage and attract industrial stakeholders. As mentioned, BSIMM is only based on observations and it is not prescriptive. This is very important since the main message for industry that wants to join this community is not “you should do it this way”, but more “compare yourself against the rest”. It seems like a clever motivation and it avoid direct judgements.

Being very good in one activity might not necessarily mean that your SDLC is optimal. For example putting lot of money on penetration testing is proved to be wrong since it will only detect few vulnerabilities. Combining all activates BSIMM gets a number of graphs which show more or less profiles per domain or area. This can be considered as “de facto” standard. Gary McGraw presented “12 things everybody does” (actually 66% is doing it):

1. Identify gates.
2. Know PII obligations.
3. Awareness training.
4. Data classification.
5. Identify features.
7. Review security features.
8. Static analysis tool.
9. QA boundary testing.
10. External pen testers.
11. Good network security.
12. Close ops bugs loop.

Activity graphs or “snowflakes”, as he calls them, can be also used for comparison purposes, for example financial industry versus independent software vendors. These “measuring sticks” are, depending on activities selected, sort of profile that might be useful for NESSoS. There is an assumption that each activity makes code better and therefore BSIMM does not try to enter into the quality of activities. However, metrics are very important to explain its goals in quantitative terms. One such metric could be security defect density. A reduction in security defect density could be used to show a decreasing cost of remediation over time. When it comes to metrics and profiles, risk appetite should also be taken into account. List of vulnerabilities
such as CWE and their priority ratings are not very useful for organisations since they do not take into account particular type of business, operational setting or risk appetite.

2.3 Industrial Presentations

Pascal Bisson (Thales) started the block of European Industry. He focused on Future Internet Public Private Partnership (FI-PPP) and FI-WARE project that deals with the Future Internet core platform. Pascal is leading WP8 in this project which is work package dedicated to security.

The goal of the FI-WARE project is introducing an innovative infrastructure for cost-effective creation and delivery of services, providing high QoS and security guarantees. The key deliverables of FI-WARE will deliver an open architecture and implementation of a novel service infrastructure, building upon generic and reusable building blocks developed in earlier research projects. This infrastructure will support emerging Future Internet (FI) services in multiple Usage Areas, including those covered by NESSoS (e-Health and Smart Grid).

From an architectural perspective, FI-WARE is based on the following main foundations:

- **Service Delivery Framework**: the infrastructure to create, publish, manage and consume FI services across their life cycle, addressing all technical and business aspects.
- **Cloud Hosting**: the fundamental layer which provides the computation, storage and network resources, upon which services are provisioned and managed.
- **Support Services**: the facilities for effective accessing, processing, and analyzing massive streams of data, and semantically classifying them into valuable knowledge.
- **IoT Services Enablement**: the bridge whereby FI services interface the Internet of Things through heterogeneous, resource-constrained and ubiquitous devices.
- **Interface to the Network and Device**: the open interfaces to networks and devices, harmonizing the connectivity needs of services built on top of the platform.
- **Security**: the mechanisms which ensure that the delivery and usage of services is trustworthy and meets security and privacy requirements.

A key element of the Core Platform has been named “Generic Enablers” (GE). These are a set of technologies offering capabilities and functionalities which can be flexibly customized, used and combined for many different Usage Areas. The generic enablers exposed by it will provide all relevant services in a standard and open format (e.g. REST, WSDL). In other words, GE is a functional building block of FI-WARE. Any implementation of a GE is made up of a set of components which together supports a concrete set of functions and provides a concrete set of APIs and interoperable interfaces that are in compliance with open specifications published for that GE.
Apart from built-in functionalities FI-WARE will offer to deal with generic concerns (e.g. Identity Access Management and Privacy) it will also offer some unique security features, such as the vulnerability interdependencies analyser tool (associated with attack graph technology) that will be used to build a complete map showing all possible paths of attack, to reduce the vulnerabilities, decrease the level of risk and to optimise security sensors placement and intrusion alert prioritization, taking into account the need to secure by priority more sensitive and more strategic services.

In continuation, Pascal Bisson presented WP8 with the main security features. The overall ambition of the Security Architecture of FI-WARE is to demonstrate that the Vision of an Internet that is "secure by design" is becoming reality. "Secure by design" is possible for the most important core (basic) and shared (generic) security functionalities in accordance with the requirements of external stakeholders and users such as the FI PPP Usage Area projects. This concept therefore addresses both the security properties of the FI-WARE platform itself and the applications that will be built on top of it. The basic security architecture will be designed to be extensible to meet these additional security requirements coming from both the FI-WARE project (development and research activities, market analysis and consortium-specific exploitation requirements) and the FI PPP Usage Area (UA) projects and their trials.

The high level architecture is formed by four main modules: Security monitoring mechanisms, a set of General Core Security Mechanisms (e.g. Identity Management and Privacy solutions), Context-Based Security and Compliance where an enhanced version of USDL (Unified Service Description Language) [7] for security will support the matching of security goals with available security services while addressing compliance management, and a set of universally discoverable Optional Generic Security Services that will be instantiated at runtime and can be dynamically reconfigured based on the needs of specific scenarios.

The most interesting for NESSoS audience was probably FI-WARE proposal to use USDL-Sec to describe security and compliance solutions. USDL-Sec documents will contain all necessary information in order to allow binding security and compliance end-user requirements, trace them and to validate solutions against these requirements.

The specific framework helps searching and browsing a large catalogue of USDL-Sec descriptor documents, in order to find the most appropriate one to fulfill the Security and Compliance requirements from the end-user environments, and to deploy it into the target system. Additionally, at runtime, USDL-Sec descriptor documents are used by the Secure Monitoring infrastructure in order to detect anomalous behaviour or non-conformance, and initialise compensation actions for the automated adaptation of the deployed security mechanism to the changing context conditions. One of the interesting recommendations for NESSoS community would be to study and compare USDL-Sec. Finally, Pascal underlined necessity to collaborate with NESSoS and presented Open Call that FI-WARE launches in 2012.
Jan Stijohann (Siemens) who was replacing Jorge Cuellar (not able to assist due to personal circumstances) gave the next presentation. Presentation started with the statement about how life has changed from “walled garden” systems into open, complex and composed systems where trust is an important enabler and multilateral security is a must. Jan Stijohann explained how Siemens deals with challenges throughout all software development lifecycle and even after it (during the operation phase). He went through challenges in each phase (plan, define, build, operate) and illustrate it with an example from Smart Grid usage area and attack called Comodo, named after Comodo Group, Inc. a privately held group of companies providing computer software and SSL digital certificates. On March 15th, 2011, Comodo reported that a user account with an affiliate registration authority in Italy had been compromised which was used to create a new user account that issued nine certificate signing requests.

The presentation focused on challenges in Service security. In the Comodo hack vulnerabilities were exploited to perform privilege escalation, to found DLL at Energy Supplier partners site that had password “hardcoded” in it, to extract these password an finally to impersonate Registration Authority (RA) and obtains certificate for Energy Supplier and finally attacker impersonates Energy Supplier to access Smart Meter and switches it off. It finally comes to the fact that the Registration authority server, that used DLL where credentials were stored in unsecure way, is an asset for energy supplier even they do not have control over it. The Comodo company believes the attack may have been an effort by the Iranian government to spy on dissidents using, but in addition to opening discussions of possible government spying and attack attribution, the situation also has turned a spotlight on one of the basic issues of the software based services and design flaws such as hardcoded authentication in an asset that makes part of Energy Supplier trust chain. This is an example how service security and corresponding risk assessment (CORAS tool was used for illustration of this example) differs from “traditional” risk assessment used in software security where control over assets is with single organisation.

The next example was dealing with definition phase and the problem of finding adequate measures. Here illustration was based on Needham–Schroeder protocol intended for use over an insecure network. This protocol is vulnerable to a man-in-the-middle attack. If an impostor X can persuade A to initiate a session with him, he can relay the messages to B and convince B that he is communicating with A.

For the building phase, example was using the metaphor of two bicycles. If they are locked in two different ways (one locks front wheel, the other one back wheel) they seem both secure enough. However, taking different parts from each bicycle (front wheel from one and back wheel from another), thief might be able to compose full bicycle. In another words, securing one service in composition of services is not enough.

Finally, Jan Stijohann commented that Siemens invests a lot in operation phase security since it is important to assure there are no vulnerabilities left even after service is built and put in the operation.
Theo Dimitrakos (British Telecom - BT) gave a presentation focused on Cloud Service and their security. There are many initiatives and frameworks in this field such as NIST, Cloud security alliance (CSA) or CAMM (common assurance maturity model) initiative. All of them mention security as the key enabler towards 2020. Theo presented security challenges and then focused on three main areas:

- **Multi-tenancy (shared infrastructure) challenges that include:**
  - Shared resources.
  - Poor Process isolation.
  - Data Segregation.
  - Data Sharing.
  - Data Erasure.
  - Data Co-mingling.

- **Technology Risks challenges that include:**
  - Hypervisor vulnerabilities.
  - Integration of security technologies complex.
  - Few cloud specific security solutions.
  - Defence in depth – is complex to achieve.

- **Finally, challenges related to security delivered at multiple layers:**
  - Virtual image provided by IaaS provider.
  - Platform stack provided by PaaS.
  - SaaS application security.

In order to deal with these three groups of challenges, BT uses direct innovation downstream. For the other group of challenges (resilience and availability, data location and mobility, information assurance and compliance) BT tries to influence European and UK policy makers, agencies or expert groups. Finally, for dealing with challenges such as cloud vendor lock in or corporate risks BT prefers to act together with other industry bodies through organisations such as Cloud Security Alliance (CSA) or Information Security Forum (ISF).

An example is BT involvement in CAMM as a framework to transparently rate and benchmark the capability of a selected solution to deliver information assurance maturity across the supply chain. The newer, the more complex, the more proprietary and the less transparent the underlying technology is, the less likely it is that a process-based evaluation will identify all of the risk-relevant considerations. Certifications such as ISO 27001, and especially SAS 70, are not up to the task of determining whether a complex cloud infrastructure has been designed and built in a secure fashion, and they cannot fully identify, let alone assess, the unique operational considerations of new environments. BT is playing an active role in CAMM with three people involved (BT leads the Operations Domain Controls authoring team).

Furthermore, Theo showed 4 directions for research in cloud security: enterprise wide use of cloud, secure access and improved governance, in-cloud security and Optimisation of choice and offering according to the SLA.
Cloud infrastructure sits on traditional network – you still need the old fashioned security controls in place. Key technology is the hypervisor, multi-tenancy, virtualisation layer and elastic compute.

In cloud security research and innovation downstream, BT received UK IT Industry awards for VHE-Cloud (secure virtual hosting in the cloud) and cloud service broker, while inside of application security they have an authorisation solution that was also a finalist in this competition. Other areas of research include authorization, in-cloud esb fabric, in-cloud content analysis, malware detection, confidentiality enhancement etc. BT also collaborates in many other initiatives such as ENISA and has many relevant publications in this area.

A different perspective on solving security problems was also presented with few examples. Issues with traditional protection methods include context intermingling of protection engines that run in the same context as the malware they are protecting against. Better context management is needed through:

- Protection by running outside OS.
- Isolated from most malware.
- Dependent on smaller, trustable codebase of hypervisor.

Other detailed examples of best practises were given, for example for secure data sharing in the cloud.

- Context-aware secure sharing of data volumes by virtual machines and applications on them.
- Encrypted cloud storage is offered ‘as a service’.
- Customer in control of connection, protection and access to their secure virtual storage.
- Keys and policy server are off the cloud data host.
- Decryption only possible when data is used in a specific “safe” environment following policy-based approval.
- Security enforced by “sand-boxed” context-aware intelligent agents embedded in customer’s VM.

2.4 Panel

The industry seminar finished with a panel dedicated to the interplay between industry and academia and the ways to improve existing collaborations. The panellists were asked to give their opening statements, followed by moderated discussion. Finally they have been asked to make final comment or closing statement. In addition, some participants provided written contribution focused on panel questions.

Domenico Rotondi (TXT) presented its company that participates, among other, in SHIELDs project.
TXT activities in secure software engineering are for:

- Internal purposes (maintenance and improvement of TXT SW platforms),
- External needs. For example, they provide SW Quality Assurance services

TXT SW development process is ISO certified and Domenico Rotondi explained that they use internal tools such as Perform Suite and Next BU for development purposes.

An application’s component **normally** does what it is expected it has to do, but for **abnormal** situations the (whole) application has to **gracefully** move to a predefined safe state (e.g. controlled termination / controlled crash).

- TXT SDLC is based on Microsoft Trustworthy Computing Security Development Lifecycle and is adopted for all products’ major releases.
- For certification of TXT products Microsoft Industry Builder Initiative (IBI) is used. TXTDemand for example is certified since 2006.
- In addition, Microsoft Dynamics Industry Solutions program (MDIS) is used: TXTPerform 2008 certified since 2009.

In 2005 Microsoft changed the procedures of its business partnership programs. MS revised the procedures to specifically address security aspects, requiring not only that these aspects had to be taken into account during the whole development process, but also that SW applications to be inserted within its business partnership programs undergo specific certification procedures. TXT was therefore forced to revise its development process to conform to MS new procedures.

The main comments Domenico Rotondi brought forward were that SW (& service) Security still perceived as an add-on, the lack of know-how on security issues by designers/developers and the lack of actual KPIs for RoI.

Valerie Issarny (INRIA) agreed with Domenico Rotondi that security used to be add-on. In matter of fact, it was an academic research perspective that “Security is key and should not be an afterthought in the overall software development process”. The other way around, leading to security-centric work is also not desirable. However, new community and new attitude is now slowly emerging.

Valerie Issarny mentioned that service engineering has focus on software service engineering and therefore secure service engineering concerns are not much different than software engineering concerns. This view was later compared with opinions from Domenico Rotondi and others which recognize that the main distinction is in security requirements which are spread over various actors.

Finally, Valerie Issarny mentioned that there is a win-win opportunity: from research to industry we should be applying and making evolve new concepts, while from industry to research there is potential of bringing in challenging and actual use cases.
Mass Lund (SINTEF) presented several examples of wrong or inexistent use of risk assessment.

- In October 2010 it has been discovered that the internal network of the Norwegian Government used for distribution of unclassified information was hacked. Several hundred thousand documents have leaked. Report of the Office of the Auditor General of Norway mentioned "The Government Administration Services [the operator of the network] has not made systematic risk assessments of the network."

- Telenor, a semi-governmental telecom company and Norway's biggest operator reported on 10 June 2011 that the capacity of speech, SMS, and GPRS in Telenor's mobile network was considerably reduced in the whole of Norway for nine hours. The cause of the incident was the restart of two central 3G nodes. Report of the Norwegian Post and Telecommunications Authority mentioned: "Telenor has not documented or described procedures to be followed and risk assessments to be made before disconnection and restart of nodes."

- Another example given by Mass Lund was about Akershus University Hospital (Ahus), one of Norway's biggest hospitals. On 19 June 2011 the internal network of the hospital is down for 14 hours (because of problems with a switch in the network). Electronic health records were unavailable (and had to be printed and distributed on paper). Because the hospital uses IP telephony, all internal and external telephone lines were also down. The hospital's report on the incident mentions: "A risk assessment of the technological solutions must be made."

- The final examples was about the Oslo water authority in September 2011 when they discovered that the facility providing drinking water to 90% of Oslo can be accessed and controlled via Bluetooth on a mobile phone and the password 0-0-0-0. Report of the Office of the City Auditor mentioned "The Agency for Water and Sewerage Works did not have sufficient focus on information security in and surrounding the system for remote control and did not have a formalized approach for the handling of the system."

These 4 examples have something in common: companies and public administrations do not apply existing solutions. So the problem might not be in what we need to investigate or the next new solution, but rather why they do not use the existing solutions in the first place. Risk assessment and management should have a more visible position and tools produced by academia deserve more visibility. However, it is sometime difficult to get 15-20 use cases to make a really good product and to build some reputation. Here is where industry-academia interplay might come into game. Another proposal from Mass Lund is involvement of government authorities in a sort of "laboratory" for risk assessment, assurance or certification.

Panel conclusions.

Final discussion was moderated by Aljosa Pasic and included questions from audience.
All panellists have also received a number of questions in advance. Some of these questions have been addressed in their position statement and some of them have been discussed in discussion afterwards. There were different opinions about link between software security and service security.

Secure Service Engineering is, in some way, less than Secure System Engineering (having to focus on specific aspects instead on the whole system security), but it goes deeper into the security of a specific component: “service”. As such it is a positive push; on the negative side there could be, could be (that doesn’t mean there will be), the risk to further consider security issues as an add on to the software development and deployment. While it is clear that software based services and their security have to be based and learn lessons from software security the main issue, it has been discussed, is to defined these “deltas”, that is issues and challenges and that make difference such as composability and risk allocations. While assurance process for the determination of software trustworthiness can be managed internally, the similar process for service trustworthiness might need to be managed and linked to a certification by a third trusted party, such as a government owned or sponsored lab. Only in this way would service security capabilities be able to be measured, compared or integrated. The government “sponsorship” for this service certification could be based on examples Mass Lund gave or could emerge from industry initiatives or even projects (e.g. Assert4SOA project).

Government involvement is also something linked to cultural bias, for example in case of USA and European industry. This cultural bias and differences are also existing in assurance processes within different European countries. In addition each sector has its own needs and attitudes when it comes to assurance or risk appetite and attitude. It is obvious that one SDLC does not fit all in the same way that one assurance process would not be feasible for all sectors. As BSIMM shows, financial sector and independent software vendors (ISV) are leading the way, but the other sectors and applications such as embedded system or critical infrastructure software should also be measured.

Another part of discussion focus on return on security investment and how to sell secure service engineering. Rather than making “new” money directly the message should be that rework and poor security leads to losses in already gained contracts. Managing risk and cost issues in SSE is still relying on empirical approaches. There are still a lot of subjective elements in evaluating threats and risks. Secure Service Engineering could provide a more objective and systematic approach in evaluating and managing risks and costs, it has been concluded. Application criticality is currently the major driver in applying some sort of a security aware approach in the application development. This is not the right direction since security aware development process has to be always there, while application criticality has to impact only the assessment of the risks and the identification of security threats countermeasures/mitigations.

When it comes to industry and academy collaboration an example given by Domenico Rotondi includes high level languages and development framework that perhaps do not generate the most efficient run-time code, but they substantially improve developers’ productivity. This can constitute an example extendible to the SW security area. Having security aware methodologies,
supporting technologies and frameworks can substantially improve both developers’ productivity and application reliability. As for high level languages and development environments this implies developers have to learn how to use them, and this is another input industry needs from academy.

2.5 Conclusions

The overall experience of this first industry seminar is very positive since it raised very interested discussions and issues related with the main topics addressed by partners of the NoE. From the point of view of dissemination, it has been an excellent opportunity to meet with people from other communities, promoting collaborations and increasing the visibility of the NoE.

In addition, several participants of this event raised various interesting recommendations to be studied or adopted by the NoE that shall be presented to the next GA.

Gary McGraw recommended to make NESSoS network and service security more attractive for industry participation (e.g. descriptive not prescriptive, measuring sticks etc) in order to increase collaboration and be coordinated with similar efforts and search for synergies. In the same line, BT recommended to cluster challenges into groups and choose the best strategy on how to address them.

FI-WARE recommended the collection and use of generic enablers and USDL-Sec in NESSoS deliverables.

Siemens proposed the use of its presentation to find nice examples that illustrate service security particularity for each phase of SDLC. SINTEF proposed the exchange of use cases for free assessment between industrial stakeholders and academia. Also they suggested to contact government and standardization bodies in order to involve them in NESSoS community.

TXT strengthened the importance of introducing software security in academic curricula as well as in lifelong learning and specialized trainings for industry.

3. Ongoing Standardization

So far, the progress in standardization activities has not been huge. The main difficulty during this first period being waiting for the different methodologies, languages and tools coming out from the different partners before being able to evaluate which kind of standards could be of interest.
Still, Aljosa Pasic, as leader of the NESSoS IAB has contacted CEN [3] and AENOR organizations [4].

Within CEN, its Innovation Department helps to develop new businesses and promotes the use of standards and CEN Workshop Agreements in new markets and those business environments that do not use them. It is of particular interest for NESSoS since the survey presented in D 14.2 shows that no standard or best practices are really in place in industry for the development of Secure Software and Systems. Also, since new modeling languages are proposed by NESSoS partners in WP7, it could be also explored if parts of them could be of use or inspiration for the ongoing standards and viceversa.

AENOR has a specific division for promoting the effective management of information security. AENOR is enabled to provide certifications of Information Security Management Systems in accordance with UNE-ISO/IEC 27001. This certification helps a company to promote data protection in organizations, improving their image and generating confidence among third parties. With respect to ISO/IEC 27001, we plan to survey to which degree companies related to NESSoS are adopting these normative rules and procedures.

In addition, NESSoS industrial partners had also meetings with other associations and industry initiatives, e.g. OWASP, Cloud security alliance and OASIS. The Open Web Application Security Project (OWASP) is an open-source application security project. The OWASP community includes corporations, educational organizations, and individuals from around the world. This community works to create freely-available articles, methodologies, documentation, tools, and technologies. We think that NESSoS CBK is aligned with the OWASP spirit so we will explore with them the possibility of linking our wiki so it can serve as a more specialized contribution to the OWASP Glossary where other fundamental security terms, problems and methodologies are explained by the OWASP community.

OASIS is a not-for-profit consortium that brings people together to agree on intelligent ways to exchange information over the Internet and within their organizations. Concerning OASIS open standards, NESSoS outputs are obviously more related to those under the topic “Security” and the topic “Privacy/Identity”. For the second period of the project we plan to align NESSoS proposed methodologies with some of these standards. On the one hand, we plan to identify possible contributions of NESSoS partners to these standardization processes or possible extensions of partners methodologies by considering some of the concepts contained in these standards.

Among de-facto standards like Microsoft SDLC, CLASP or BSIMM, we contactive a representative of BSIMM which presented this descriptive (not prescriptive) methodology to NESSoS partners. We will try to have experts presenting the other methodologies in the following industry seminar since we aim to present standard alternatives to increase the awareness of industrial partners and promote their adoption among them.
4. References

Annex A: Terms of Reference First Industry Seminar

Date: 28th October 2011
ServiceWave 2011, Poznan (Poland)

First NESSoS Industry Seminar

Secure service engineering: from best practices to scientific excellence (and vice versa).

http://servicewave.eu/2011/workshops/

Organizers’ Names and Affiliation

Aljosa Pasic (Atos Origin): aljosa.pasic@atosorigin.com
Fabio Martinelli (CNR): Fabio.Martinelli@iit.cnr.it
Jorge Cuellar (Siemens): jorge.cuellar@siemens.com

Workshop theme, goals and relevance

The domain of Engineering Secure Software Services covers a collection of engineering activities that aim for the creation of software services – i.e. ICT services delivered through the deployment of software systems- that are both behaviorally correct (typically guided by software engineering principles) as well as secure. The specific engineering activities range from requirements engineering and analysis, over the creation of architectures, high-level and detailed design into implementation through the reuse and composition of existing artifacts, as well as through the programming of new entities, typically components and services.

In practice, industry is often faced with cost and time constraints, which leads to implementation of “best efforts” or “reasonable” security. However, security challenges are continuously evolving and the complex nature of the Future Internet is stressing the importance of comprehensive and systematic approach to secure software and service engineering. There is a demand for a set of new engineering methodologies, tools and techniques as well as methods to provide justifiable evidence and assurance for security while retaining in mind the constraints related to effectiveness and cost-efficiency. There is, however, a possibility for exploiting synergies of advanced research approaches with industrial best practices in order to reduce the gap between theory and practice, and to pave the way for the future secure software and service engineering.

In the framework of NESSoS project, we are planning to organize a series of workshops on secure software engineering focused on this interplay between industry and academy. The First NESSoS industry seminar, collocated with
ServiceWave 2011, is organized not only with the purpose to introduce the project to the industrial community, but also to collect and analyze industry best practices, current needs and upcoming challenges. Prior to this industry part, scientific community representatives from NESSoS will introduce project and state of the art.

This workshop therefore intends to allow more structured interaction between industrial and scientific stakeholders in the field of secure engineering of software and services. For this reason, it is planned to invite the most relevant industry actors to present their best practices from diverse application areas in order to analyze several perspectives. It is expected to identify future key challenges to address in the field, in particular in the context of the evolution towards the Future Internet, as well as directions for scientific community which should align future research with the industrial needs.

On the other hand, this workshop will also support the spreading of the academic research excellence in software engineering to the industrial stakeholders. This will, as well, contribute to increase the trustworthiness of the Future Internet core platform and services and will help to raise the awareness about the importance of taking security requirements into account from the very early stage of design. The principle of addressing security issues from the very beginning is contributing to reduce system and service vulnerabilities, improve the necessary assurance level, thereby considering risk and cost issues during development in order to prioritize investments.

Finally, this workshop aims to identify trends that create market opportunities, both technical and economic, and to create exploitation opportunities.

As output of this industry seminar, a report will be published with a twofold objective: it will not only serve as a communication tool to transfer knowledge, but it will also provide useful feedback to quantify the effectiveness of the seminar in relation to its objectives and take measures for future events. In addition, this seminar results will be integrated in the NESSoS public repository to grant it more visibility.

**Organization**

ALJOSA PASIC current position is Public Sector Director of Atos Research & Innovation (ARI), based in Madrid, Spain. He graduated Information Technology at Electro technical Faculty of Technical University Eindhoven, The Netherlands, and has been working for Cap Gemini (Utrecht, The Netherlands) until the end of 1998. In 1999 he moved to Sema Group (now part of Atos Origin) where he occupied different managerial positions. During this period he was participating in more than 50 international research, innovation or consulting projects, always related to the areas of information security or e-government. He has also been involved in the work of many international organisations such as ENISA, ERCIM, NESSI, EFIA, EOS, IARIA or IFIP. His current interests include Secure Software Engineering (e.g. the chairman of NESSoS industry advisory group), electronic identity (e.g. involvement in thematic network SSEDIC) and privacy (e.g. member of the advisory board of Trust in Digital Life initiative).
FABIO MARTINELLI is a senior researcher of IIT-CNR where he leads the information security group. He usually manages R&D projects in ICT (also with industrial partners) with an overall budget of several millions EURO. He also participated as security expert on the winning bid by IIT-CNR and other partners to set up the EURid consortium for managing the “.eu” registry. He has also a significant experience on running EU projects, in particular, he has been involved with several leading roles in the following FP6-FP7 projects: ARTIST2, BIONETS, CONNECT, CONSEQUENCE, GRIdtrust, S3MS, SENSORIA. He is active in community building efforts. He founded and managed the WG on security and trust management (STM) of the European Research Consortium in Informatics and Mathematics (ERCIM) since 2005 till 2009 and he is involved in several Steering Committees of international WGs or Conferences/workshops. He serves as PC-chair/organizer in several international conferences/workshops. He is the co-initiator of the International Workshop series on Formal Aspects in Security and Trust (FAST), one of the first events to recognize the necessity to consider trust and security issues altogether in new virtual and dynamic organizations/coalitions. He has a specific expertise on running summer research schools on topics related to computer security. In particular, he is serving as scientific co-director of the international research school on Foundations of Security Analysis and Design (FOSAD) since 2004 edition.

JORGE CUELLAR is a principal consultant at Siemens AG. He was awarded the DI-ST Award for the best technical Achievement for his work on modelling of operating systems and transaction managers. He has co-authored about 30 papers on different topics, including mathematical modelling of performance analysis, on learning algorithms, hand-writing recognition, formal specification and verification of distributed system design, and security. He has done technical standardization work, related to the development of privacy and security protocols at the IETF, 3GPP, and the Open Mobile Alliance. He has 16 inventions and patents. He has worked in several EU funded research projects, in particular in AVISPA and AVANTSSAR, both related to the formal modelling and verification of security and currently in NESSoS, WebSand and SPACIoS. He has served in many Program Committees in international conferences, and in particular he has been the PC Co-Chair of SEFM (Software Engineering and Formal Methods in 2004), FM’08 (Formal Methods in 2008), and STM’10 and in the steering committee of ESSoS. He has presented more than 20 invited talks at conferences and seminars, and acts regularly as a reviewer for international conferences and journals. He has been in the editorial board of Journal of Science of Computer Programming – Elsevier, and has been guest editor in several journals. He is a member of the Industrial Curatory Board of Dagstuhl, Leibniz Center for Informatics, the world’s premier venue for informatics. He has held many short term visiting teaching positions, in different Universities around the world.

**Workshop Format and Length**

This is the first seminar out of the four to be organized by NESSoS and its estimated duration is half a day. Participation of the other experts from scientific community of NESSoS and S-Cube including University of Duisburg-Essen and
the French National Institute for Research in Computer Science and Control (INRIA).

The structure of the workshop will revolve around the following parts:

- **Introduction and NESSoS project presentation (30 minutes):** Welcome to the audience and introduction of NESSoS objectives, status and results achieved during the first year. Fabio Martinelli (CNR), as NESSoS project coordinator, will be leading this section of the workshop.

- **State of the art and scientific advances (30 minutes):** This section will analyze the current state of the art on Engineering Secure Software Services by academy actors and last advances on this topic.

- **Industry keynote (30 minutes):** Keynote address from industry representatives. Atos Origin and Siemens, but also NESSoS Industry Advisory Board members will be invited to participate. This session will be moderated by Jorge Cuellar (Siemens).

- **Coffee break (30 minutes).**

- **Panel with 4 speakers plus open discussion (70 minutes):** A panel made of industry and academy actors will be invited to participate. The discussion will be focused on current needs and future challenges and on how the community is able to address them now that Future Internet is near to become a reality. This panel will be chaired by Aljosa Pasic (Atos Origin) who will open a 20 minutes open discussion where the audience will be asked to join the debate.

- **Conclusions and future activities (20 minutes):** This last block will close the workshop wrapping up the most relevant conclusions and summarizing which are the future steps to go forward.

**Estimation of Attendance**

The estimation of participants in the seminar is around 30 people. Among other relevant participants belonging to the Secure Software Engineering community, NESSoS Industry Advisory Board (20 organizations) plus members directly (10 partners) or indirectly involved in NESSoS project (5 associated partners) will be invited to take part of the seminar. The organization will encourage both the industry and academy participation in order to make sure the workshops’ participation is well-balanced.

**Information about Past Workshops**

In 2008, the ERCIM together with the EC DG INFSO Unit F5, organized the “2008 EC- ERCIM Seminar on ICT Security – Engineering Secure Complex Software Systems and Services” in Brussels.

**Advertising**

This workshop will be advertised in NESSoS webpage and it will be announced though the NESSoS mailing lists to the network of excellence. The seminar will
be also disseminated to the Future Internet community though Effects+
channels of dissemination.

**Agenda**

9:00 – Introduction - **A. Pasic** (AtoS).

9:10-9:30 NESSoS Project overview - **F. Martinelli** (CNR).


10:15-10:30 Coffee break.

10:30 -11:00 Challenges of secure service engineering – **J. Cuellar** (Siemens).

11:00-11:20 Generic enablers for security of Future Internet Services – **P. Bisson** (Thales).


11:40-12:50 Panel.

- **Aljosa Pasic** (ATOS) – Moderator.
- **Valerie Issarny** (INRIA).
- **Mass Lund** (Sintef).
- **Domenico Rotondi** (TXT).

12:50-13:00 wrap up.