Automated VAlidatioN of Trust and Security of Service-oriented ARchitectures

FP7-ICT-2007-1, Project No. 216471

www.avantssar.eu

Deliverable D1.7
Technology Implementation Plan (TIP)

Abstract

This deliverable explores the opportunities for exploitation of the results of the AVANTSSAR project; this includes use of the research for both the academic context and the industrial context. The deliverable describes intended exploitation by the project partners, as well as public dissemination of the results to give other parties, such as academic institutions and organizations from different business domains, the opportunity to employ and build upon the technologies that have been developed in the context of AVANTSSAR.

Deliverable details

Deliverable version: *v1.0*
Classification: *public*
Date of delivery: *03.01.2011*
Due on: *31.12.2010*
Editors: *all*
Total pages: *45*

Project details

Start date: *January 01, 2008*
Duration: *36 months*
Project Coordinator: *Luca Viganò*
Partners: UNIVR, ETH Zurich, INRIA, UPS-IRIT, UGDIST, IBM, OpenTrust, IEAT, SAP, SIEMENS

Contents

1 Introduction

This deliverable explores the opportunities for exploitation of the results of the AVANTSSAR project; this includes use of the research for both the academic context and the industrial context. The deliverable describes intended exploitation by the project partners, as well as public dissemination of the results to give other parties, such as academic institutions and organizations from different business domains, the opportunity to employ and build upon the technologies that have been developed in the context of AVANTSSAR.

1.1 Scope

The scope of this implementation plan includes all the technologies that have been produced within the project and the intended use of this research upon completion of the project. This includes strategies for dissemination of the research to academic, industry and standardisation bodies (described in more detail in [2]), as well as exploitation of the technology by project partners for their own purposes. This deliverable will not detail specific implementations of the research by parties external to the project consortium.

1.2 Objective

The primary objective of this deliverable is to develop key strategies for exploitation of the research to achieve the greatest benefit for all stakeholders. Migrating project results to industry and standardization organizations will speed up the development of new network and service infrastructures, enhance their security and robustness, and increase the public acceptance of emerging IT systems and applications based on them. We also aim to promote the utility of formal validation techniques in secure application development fields.

1.3 Content

In Section 2, we give a brief description of the project and its results. Section 3 explores market environment characteristics, trends and key players relevant to this research and commercialization of the results. Section 4 then describes the high-level approach to employing the project results. Finally, Section 5 contains a number of individual exploitation strategies for the different partners in the project, defining their specific plans for implementation of the technology.

2 Project Description

In this section, we give a brief description of the project and its outcomes, so as to provide a common understanding of the concepts that are the subject of this technical implementation plan. More information can be found in further project documentation.

2.1 Project Scope and Vision

In today's rapidly change business environments, technologies and requirements are quickly evolving. IT systems and applications are undergoing a paradigm shift where components are being replaced by services, distributed over the network, and composed and reconfigured dynamically to meet current organizational demands. This trend of organizations moving to service-oriented architectures has shown significant benefit to organizations and is set to continue for the foreseeable future.

Due to the distributed nature of service-oriented architectures, exposing services in future network infrastructures entails a wide range of trust and security issues. Resolving these issues is exceptionally challenging because simply ensuring each of the service components are trustworthy is insufficient; composing services leads to new subtle and dangerous vulnerabilities due to interference between component services and policies, the shared communication layer, and application functionality. As a result, a method to validate both the service components and their composition into secure service architectures is needed.

AVANTSSAR proposes a rigorous technology for the formal specification and automated validation of trust and security of service-oriented architectures. This technology has been automated into an integrated toolset, the AVANTSSAR Validation Platform, which has been applied on a number of relevant industrial case studies.

The primary outcomes from the project, which will be the subject of this implementation plan, include:

- ASLan, a formal language for specifying trust and security properties of services, their associated policies, and their composition into service architectures.
- Automated techniques to reason about services, their dynamic composition, and their associated security policies into secure service architectures.

- The AVANTSSAR Validation Platform, an automated toolset for validating trust and security aspects of service-oriented architectures.
- A library of validated composed services and service architectures, proving that the technology scales to envisaged applications.

2.2 Project Objectives

The primary objective of this project was to work towards the possible future establishment of an industry standard for automated validation of trust and security of service-oriented architectures.

2.3 Project Approach

The project consortium took a strong collaborative approach to this project with relevant contributions made by all partners. This afforded the opportunity to leverage the unique abilities of both the academic and industry partners. Each partner made contributions in a manner that was beneficial to both the project and their individual organization. The purpose of this was to ensure that worthwhile and implementable results were produced, which would be viable in real-world contexts. Each partner has the right to commercially exploit the research they have produced, free from intellectual property limitations which might otherwise limit implementation activities.

2.4 Project Use Cases

The AVANTSSAR Library of validated problem cases [3] contains a number of validated composed services and service architectures that illustrate how the AVANTSSAR languages and tools can be applied on industrially relevant use cases. As an example in the eBusiness domain, we can consider a version of the Loan Origination Process (LOP), which is the process a bank uses to assess customer loan applications. This offers the possibility to focus on workflow security aspects to verify the ability of the platform to identify unexpected behaviors in the interplay between the workflow and the access control policies. Within such processes, access control is very important to ensure that applications are processed fairly and without bias. Using ASLan, one can formalize the process as well as the security requirements for the process, for example ensuring the separation of tasks to different actors in the process or with-holding of personal identification information when actors are assessing the viability of the loan candidate. Given this specification, the

AVANTSSAR Platform can then be used to analyze the enforcement of the security controls.

3 Market Analysis

This section explores the market environment relevant to AVANTSSAR. It examines IT security in general and, in particular, the SOA environments, including current practices for organizations operating in this environment to identify where AVANTSSAR fits in and can be used.

3.1 General Market Overview

The purpose of this market analysis is to examine the market environment in which the results of the project are intended to be exploited. Broadly speaking, the AVANTSSAR technology is relevant to any organization developing and/or using SOA systems as part of their operations, in order to ensure the reliability of trust and security for these complex systems. Current practices do not include the usage of a formal method approach for validating trust and security. Instead, ad-hoc and less rigorous methods tend to be used by system architects during the design and development process, whereas post-development testing and add-on security measures or separate solutions may be used to prevent risk. The main problem with this approach is that without formal methods, vulnerabilities in the architecture can often slip through undiscovered. As a result, some organizations perceive the risk as unlikely until they experience the negative effects of an event of system failure or the exploitation of a vulnerability previously undetected. So, the cost-benefit or return on investment figures for the adoption of the AVANTSSAR approach are actually difficult to calculate or justify as the cost is dependent upon the level of adoption and usage and the value of this technology is to prevent instances of loss rather than generate tangible return. This presents a marketing problem for AVANTSSAR. In the cases in which SOA systems are highly sensitive to security and trust, and the result of a breach would be very severe, organizations are however more motivated to address the issue in a formal way. Such cases can also potentially involve highly complex systems with many components interacting and detailed security requirements, which makes the manual validation of security difficult and labour-intensive. The organizations involved in complex and/or security sensitive system development hence form the most attractive market for the AVANTSSAR technology.

The market for AVANTSSAR can also, of course, consider the academic and industry research fields, whose researchers may be interested not only in applying the technology in specialized cases but also in further developing it, perhaps even taking it in new directions.

3.2 Description of the Market

Summarizing, the AVANTSSAR project targets

- organizations engaged in activities related to SOA and model-driven software development, with the purpose of facilitating and improving business operations within organizations and interactions with their customers, where security plays a crucial role,
- academic institutions conducting research in this area or related ones,
- consulting firms providing security services to other organizations, and
- standardisation bodies, who may also influence the operations of different organizations on a large scale.

One of the primary challenges of reaching the market is the task of communicating to a broad spectrum of organizations in order to convey complex information for what may be considered a niche market. Since AVANTSSAR provides the first formal platform for automated validation of trust and security of SOAs, concern for direct competition is a lesser focus; instead, the process of facilitating acceptance/adoption of this new and complex technology is of high priority.

Industry commentators and information from a number of different providers consistently agree that a clear trend in the IT security environment is the increasing sophistication and severity of targeted security attacks [10]. As a result, organizations must work to mitigate the risk of loss of assets (IT infrastructure, applications and data), and thereby minimize vulnerability to attack. Gartner identifies vulnerability management as a key issue for organizations today, in particular, identifying the most effective technologies and best practices for discovering and eliminating security weaknesses and closing compliance gaps. Where applicable, AVANTSSAR can contribute to increased compliance as well as vulnerability management, as it can be used by developers to validate the compliance of their systems to relevant security requirements.

Further market trends identified include [9]:

- Organizations spent 5% of IT budgets on security in 2010, down 1% from the previous year. In normal times, Gartner suggests spending 3 to 6% of IT budgets on security.
  - IT security spending varies widely between organizations, due to company size, region and industry domains, as well to varying sensitivity to security (e.g., need to protect sensitive information).

  - The professional services sector seems to be spending the greatest percentage of the IT budget on security at 6.8%, whereas transportation seems to be the lowest at 2.8%.

- Gartner suggests explicit IT security spending may decrease in the future because security capabilities are increasingly bundled into network and desktop functionalities as technology improves. From this viewpoint, we can consider AVANTSSAR as helping to enable such security improvements because it allows developers to validate security controls at a much earlier point in development, and much more easily, when considering highly complex SOA systems.

According to the survey [10]

> Despite ongoing worldwide economic difficulties and broad coverage of the challenges associated with implementing SOA, nearly 100% of 411 organizations surveyed by Gartner report that they are either using SOA on some of their projects today or they expect to use SOA on some projects within the next 12 months.

The survey also reports that in many organizations, the distributed ownership across multiple organizational units of many SOA implementations poses a number of critical challenges including security.

As shown by the use of AVANTSSAR to identify and subsequently allow resolution of a severe security flaw in the protocol used by Google's SAML-based Single Sign-on for Google Apps (documented in several other deliverables), vulnerabilities in SOA systems can be easy to overlook. Prior to the discovery and resolution of the vulnerability, the flaw allowed a dishonest service provider to impersonate a user in order to interact with and gain information from another service provider the user was engaged with. In November 2010, the e-commerce provider PayPal released a fix for a significant security vulnerability in their existing iPhone application, due to the apps failure to confirm the authenticity of PayPal's website when communicating over the internet. This vulnerability could have allowed a hacker to "electronically step between a user and PayPal, pretend to be the PayPal website and gather usernames and passwords", as quoted by Naraine [23], according to the security firm who discovered the flaw.

These two instances of security vulnerabilities passing through existing development processes demonstrate how easily faults can go undetected, exposing organizations and their customers to malicious attacks.

Security attacks by hackers are not the only concern when an organization has to ensure the trust and security of a system running a business

process. For some dematerialized operations, such as the one modeled in the AVANTSSAR DCS (Digital Contract Signing) and PB (Public Bidding) use cases, threats can also come from litigation when one business party, to defend its own interest in a dishonest way, may contest in court the authenticity of a business transaction. The attacker may argue that the business process has security flaws in terms of integrity, confidentiality or non repudiation properties fulfillment, and, even if no attacks have been proven, the existence of the flaw makes the transaction void. This concern is very common when migrating from an existing process involving handwritten signatures for legal reason (half-dematerialized/half-paper process) to a fully dematerialized process. Only a few years ago, even if organizations already offered online services for subscribing to health insurance or for opening bank accounts, subscribers had to finalize the process by sending a paper contract. This prevents the process from being completed on the spot. Now, there are more and more fully dematerialized processes thanks to the use of digital signatures and generalization of digital IDs. In fact, in some European countries, such as Spain, Belgium or Estonia, personal certificates for legally recognized strong authentication are embedded inside the national e-ID card and are used by citizens for online banking and administrative transactions. This trend is not limited to Europe as the government of India oversees a national hierarchical PKI to support digital signatures to be used in business processes. AVANTSSAR modeling and validation techniques may help in formalizing the new security requirements that organizations are not accustomed with when using former processes.

3.3 Revenue Streams

In terms of options for commercial exploitation of AVANTSSAR and revenue streams, the market that was described in the previous section may not be of sufficient volume to warrant launching a standalone application. This may change in the future, however, the present (relative) immaturity of the technology and the expertise required to adapt it to different industry contexts suggest that further development of these concepts is necessary before a standalone application may be deemed viable. Having said this, there may be significant opportunities for commercialization through a consulting service model and/or training and education events.

Through a consulting service model, one or more partners may be able to work on an individual industry implementation project to adapt AVANTSSAR to an individual SOA system, for example, by building a connector to interface with the AVANTSSAR Validation Platform. As identified in Subsection 3.1 (General Market Overview), this model would suit cases where

the SOA system in question is highly complex and/or security sensitive (such that it would be very difficult to validate it manually and such that the effects of a vulnerability being exploited would be very severe). Given the knowledge and experience that has been generated within each of the partners, they are uniquely qualified to offer their expertise as a service. As such, provided a suitable and motivated candidate may be sought, the potential charge rate could be higher than average when compared to generic consultation services, which compete more on price. This unique expertise can also be applied through training and education events such as workshops, lectures, short courses, etc. Research and academic players may be interested in learning more about this technology and such events can be quite lucrative if sufficient demand can be generated and resources (expert staff, education materials and facilities) applied.

These options for commercialization are merely potential and would have to be explored in more detail by a partner wishing to engage in them, for example by developing a detailed business case. The current intentions of the partners, for use of the research, are detailed later in this deliverable.

3.4 Target Markets

The main impact targets or customer segments are research institutions, industry, and standardization bodies working on the design of web services and service-oriented architectures, focussing in particular on their trust and security aspects.

3.4.1 Research Institutions

Operating in the same sphere as the project partners, research institutions may be considered the easiest target audience to reach. Having said this, research communities can be tough critics, so it is important to follow standard research dissemination techniques including peer reviewing, publications, presentations at conferences and patent filings. Knowing this in advance, dissemination activities have been conducted throughout the project, as detailed in [2] ("Final Dissemination and Use Plan").

Generating interest in the technology across a wide network can stimulate further research in other areas of the topic, helping to improve and develop the maturity of AVANTSSAR for the benefit of all parties involved. Their support can also help to give further credibility and improve receptiveness of the other target segments.

3.4.2 Industry

While SOA solutions are being developed and used in a wide variety of industry domains, the technology is suited particularly to highly security-sensitive industries or implementations, for example e-government, e-health and e-banking scenarios where highly sensitive data is involved and the impact of a security attack is more severe. As described in the banking use case, a customer's loan application and subsequent loan origination process within the bank requires enforcement of certain security controls to ensure fair and viable assessment of the application.

Challenges in accessing this market sector include the process of motivating organizations to employ the AVANTSSAR technology given the complexity and specialized knowledge required, the current lack of substantiation by standardisation bodies and a lack of perceived need despite recorded incidents proving the contrary.

Potential gain from use of the technology, however, is the ability to deliver secure SOA systems and prevent instances such as those experienced by PayPal and Google as described previously, including the cost of fixing the error after the system has gone live, damage to company reputation, loss of customer trust and the possible damage resulting from malicious exploitation of these vulnerabilities.

Through industry migration activities that were already carried out during the project, much has been learned towards improving the technology and making it more attractive for general market adoption. SAP's proprietary implementation of an AVANTSSAR connector for its existing SAP NetWeaver BPM tool (a component of SAP NetWeaver enabling modeling, executing and monitoring of business processes) proved very successful. Using a plug-in to automate the security validation of an analyst's model created in NetWeaver BPM can be very useful. The analysts do not have to consider the complex logic and the mathematics underlying AVANTSSAR. Their only concern is specifying their desiderata and pressing a button. Though this level of seamlessness is not always achievable, there may be many other application domains where this is feasible.

Organizations are also subject to regulatory requirements related to security and trust. There are strict laws in many countries regarding the disclosure of breaches to the security of user/customer data. In the case of online SOA systems, "Terms and Conditions" statements, which customers must agree with to be able to interact with the systems, are also legally binding. Breach of these conditions by organizations, as a result of security vulnerabilities, can leave them open to litigation. European laws in general are particularly strict with regards to legally binding business processes and

highly favor implementation of strong security mechanisms like digital signature based on certificates. This is also the case for India and Latin America.

From a social perspective, trust and security is highly important to the reputation of some organizations particularly in industries such as government, health and banking. If, as a result of security flaws being discovered in their systems, a company loses trust perception with their customers this can have a detrimental effect on their core business. Even if a vulnerability is later resolved, the damage to customer relationships may already be done. Therefore the best method is to ensure the delivery of secure SOA systems before implementation and deployment.

Each of the motivating factors (economic, legal and social) and the examples of security vulnerabilities discovered in the systems of large organizations as described in this section can be used when communicating with industry in order to bring them onboard with AVANTSSAR. As this is a new technology, we are essentially establishing a new market or "blue ocean strategy", which can be a lengthy process to change long held attitudes and approaches. Therefore significant effort is required to achieve the objectives for the project in generating industry uptake.

3.4.3 Standardisation Bodies

International standards organizations such as ISO, OASIS, W3C and IEEE provide publicly available standards for use worldwide and are well known and respected across different industries. As explained by Wikipedia [24]

> Technical barriers arise when different groups come together, each with a large user base, doing some well established thing that between them is mutually incompatible.

Therefore, it is better to establish one single method to overcome such barriers and allow intercommunication and interoperability across industries. Standardisation can, however, be difficult to achieve. The reasons for such difficulty can include conflicting options or candidates, lack of adequate research, insufficient market demand or inadequate efforts to achieve it.

Alignment with and acceptance of AVANTSSAR by international standardisation bodies can drive industry adoption of the technology due to perceived independent third-party substantiation of quality, validity and benefit. Successful acceptance of AVANTSSAR has the potential to open up opportunities for consulting services for those in the project consortium with expertise to adapt the technology and potentially develop plug-ins or connectors to allow the platform to be employed in a wider range of industrial and development contexts.

3.5 Competition and Competitive Advantage

Whilst we described AVANTSSAR as the first platform for automated validation of trust and security, we can still consider that there is some competition for this technology. This includes already established SOA specification languages and ad-hoc methods and reasoning currently used to identify security weaknesses in the architecture at design time.

The AVANTSSAR languages allow specification of trust and security properties of services, their policies and their composition, which is not a new concept. There are a number of other established specification languages for SOAs and their implementation via web services. In order to produce the greatest result for the project, these languages were carefully studied to identify and learn from their advantages and disadvantages (this is documented in [1]). Languages such as XACML and SAML are widely used to effectively define security features in SOAs and as such, various technical concepts have been adapted for AVANTSSAR. The value or competitive advantage of AVANTSSAR is that it not only defines the system and its security policies, but automatically validates their enforcement throughout the SOA architecture.

Employing ad-hoc methods and reasoning to validate security when designing SOA systems may be a simpler way of approaching the issue than using AVANTSSAR, but it is much less reliable. Accuracy may depend on the expertise of the developers and the time/resources at their disposal for such a task. As demonstrated in the case of Google's SAML Single Sign-on solution and PayPal's mobile application, vulnerabilities can be easily overlooked if a formal approach is not taken. While in these cases the vulnerabilities were discovered and resolved before any damage by malicious hackers, others are not so lucky and this poses a significant risk especially when sensitive data is concerned.

3.6 Conclusion

The information identified in this section provides a thorough understanding of the target market for the AVANTSSAR technology and as a result, the strategy to exploit the technology within the market has been shaped accordingly. Examination of industry trends has demonstrated a clear and ongoing market for the implementation of the AVANTSSAR platform in different industrial SOA contexts due to continued popularity for this method of system architecture, critical concern for robust system security and the severe consequences that can result from allowing deployment of insecure systems. AVANTSSAR provides significant advantage over current languages for spec-

ification of trust and security properties of services, their policies and their composition as well as ad-hoc methods and reasoning current used to ensure enforcement of security requirements across SOA architectures. This is because AVANTSSAR automated the formal security validation process, and therefore developers can more easily detect security vulnerabilities if they exist and be more confident in the robustness of their final solutions.

Research institutions provide a wealth of opportunities to gain support for the project and drive acceptance from standardisation bodies and industry. Highly security-sensitive industries and SOA systems are likely to be more receptive to AVANTSSAR as the cost of vulnerabilities or security breaches can be detrimental to the organization.

AVANTSSAR is a quite complex and not yet fully mature technology, but there are strong legal, social and economic factors to motivate further development. New research projects (such as the FP7 project "SPaCIoS" [20], which will be carried out by some of the partners of AVANTSSAR, including the same project coordinator) and market testing (to be carried out by AVANTSSAR partners as well as project-external interested parties) would give significant benefit to this initiative.

4 General Exploitation Strategy

As the project reaches completion, all partners are confident in the results that they have produced and are therefore beginning to exploit the extensive potential value of these results. This section describes the general approach to be taken in executing the exploitation activities before delving further into the individual activities of each partner.

We do not believe that automatic tools for the security and trust validation of services will be attractive enough for a commercial market, for reasons of potential market volume and appropriate pricing. In order to best exploit the value of the research that has been produced, the results have been (see [4]) and will be further submitted to industry standardisation bodies in an effort to establish AVANTSSAR as an industry standard for security and trust validation in SOA systems. Success in achieving status as de facto standard methodology and toolset could open up a market for the project partners to offer consulting services around this technology, making use of the unique expertise developed during the project.

The technology developed in this project will also be used as a basis for the FP7 project SPaCIoS [20]. The technology will also provide value in two other EU-funded research projects that started recently, DIAMONDS [8] and NESSOS [18].[1] As much of the AVANTSSAR results will be used as a basis for these new projects, they can be considered as part of our exploitation strategy. Such further commitment to research on this subject by many of the AVANTSSAR partners shows a strong confidence in the value of the work that has been carried out and the potential to deliver further valuable research in the future.

4.1 Exploitation approach

In order to exploit the results of the project, the primary approach is public dissemination of the research, targeting industry, academic institutions and standardisation bodies. To achieve this effectively a number of activities have been planned and actually begun, including:

- Talks at relevant international conferences and forums (both presenting the technical achievements and surveying the project's objectives and

[1] NESSOS is a network of excellence that began in late 2010. It includes three partners of AVANTSSAR and focuses on a set of methodologies, processes and tools for engineering secure Future Internet software services. AVANTSSAR is mentioned in Workpackage "Security assurance for services" (lead by ETH Zurich) as a key enabling technology to be exploited within NESSOS. As a result, NESSOS can also be considered as part of the general exploitation of AVANTSSAR.

results).

- Publication of papers in proceedings of international conferences as well as in international scientific journals.
- Organization of workshops on project-related topics, including project workshops where attendance of external experts and professionals is based on invitation.
- Organization of tutorials and thematic lectures at schools.
- Design and management of a publicly available website that includes descriptions of the main project results and, in particular, the AVANTSSAR software suite and announcement of the publication via a number of mailing lists of potentially interested parties.

Further details on the conduct of these activities can be found in the Deliverable [2] "Final Dissemination and Use Plan". The purpose of these activities is to generate awareness about the project within the target market. Delivering a strong and clear message to a wide audience with a clearly communicated value proposition is intended to help stimulate market adoption of the technology. This in turn could improve chances for moving towards adoption of a de facto industry standard for this technology in the future.

Effective communication regarding the technology is also intended to generate interest within industry and organizations, so that eventually they may employ the technology within their own SOA projects. If this occurs, there may be an opportunity for project partners to engage by providing a consulting service employing the AVANTSSAR Platform. This may occur as a research based activity, to further develop the principles of the technology through feedback from real world implementation, with no consultation fee arrangement, or as a formal consultation service with partners charging organizations for their time. As planned dissemination activities have yet to be completed and there are no current candidates for this interaction model, further details on strategy and approach cannot be provided; however, the capability is in place for it to occur once candidates have been identified.

4.2 Expected Impact

The primary impact targets are industry, research institutions, and standardization bodies worldwide, working on the design of web services and SOAs, and focusing in particular on their trust and security aspects. Successful establishment of AVANTSSAR as an industry standard is likely to

result in greater industry uptake, helping organizations to deliver more secure SOA solutions within and even across industry domains. It is expected that, through use of this technology, society as a whole will ultimately benefit from the results of the project in terms of increased reliability and acceptance of, and confidence in, SOAs across all industry domains.

5 Individual Exploitation Strategies

5.1 UNIVR: Università di Verona, Italy

Partner Profile The University of Verona is one of the largest universities in the North-East of Italy. The Department of Computer Science has been ranked for several consecutive years as the first medium-size computer science department of Italy by an official analysis of CENSIS (the national centre for statistical analysis of the society). The department has almost 50 faculties covering the principal subjects of computer science, and members of the department are involved in 10 FP7 projects (5 of which as coordinating beneficiary), whereas the University of Verona is involved in more than 20 FP7 projects.

Individual Goals of Exploitation Since UNIVR is an academic partner, the main reason for participating in the project was basic and advanced research, and its application to current industrial-level problems in the validation of web services and service-oriented architectures. Moreover, UNIVR also aimed to further scale up validation techniques that it had helped develop for the formal automated analysis of security protocols in forerunner FP5 projects, and thereby develop a technology, the AVANTSSAR Validation Platform, that could be applied both for the analysis of concrete case studies stemming from industrial practice and for educational purposes. For instance, to be employed in the master-level courses on computer security offered at the University of Verona so as to help educate a new generation of computer security analysts.

Identified Exploitable Project Results UNIVR plans to exploit the AVANTSSAR Validation Platform as a whole both for industry-level applications and for educational purposes, as described in the previous paragraph. Moreover, UNIVR also plans to use the languages, techniques and backends that comprise the platform in other national and international research projects; most notably, the AVANTSSAR Validation Platform will provide a basis for the new technology that will be developed in the context of the FP7 project SPaCIoS [20].

Value Proposition As remarked above, UNIVR has been ranked for several consecutive years as the first medium-size computer science department of Italy, and this is in particular true for what concerns ICT and security. Through this project, UNIVR has acquired extensive expertise on service-oriented architectures and their formal validation, which may in future be

employed within an national industrial context to adapt the technology to the needs of a particular organization. Such activity would deliver value by further maintaining the national and regional reputation of UNIVR and contributing to it's core business of delivering industry-relevant research and education.

Value Creation In order to achieve the value proposition defined above, UNIVR will continue to apply the research knowledge, that has been gained through the project, to it's educational activities, as well as to to current and future research projects to build upon and develop the AVANTSSAR technology.

Revenue Model While at the current stage there are no specific plans or intended customers, UNIVR plans to offer paid consulting services to adapt the AVANTSSAR Platform to particular organizations. The market for such a service is however still immature in Italy, but we expect that this will change in the near future, at which point this issue and related factors such as pricing and service models will be reconsidered accordingly.

Status Report of Exploitation Activities UNIVR has already exploited the project results for educational purposes, both at the University of Verona and in two summer schools (courses held by Luca Viganò at Fosad 2009[2] and AILA 2010[3]). Moreover, the languages, techniques and tools have been exploited in the context of the Italian Prin'07 project "SOFT", which ran from September 2008 to September 2010, and work is already underway on the project SPaCIoS [20], which will exploit all the project results, scaling them up from design time to provision and consumption time. The effort here will be on extending the languages and techniques so as to allow for validation (and in particular, testing) at these later stages of the service development life-cycle, which is a considerably challenging task.

[2]Course "On-the-fly Model Checking of Security Protocols and Web Services" at Fosad 2009: 9th International School on Foundations of Security Analysis and Design, University Residential Center of Bertinoro, Italy, August 30 – September 4, 2009, www.sti.uniurb.it/events/fosad09/

[3]Course "Logica computazionale e sicurezza informatica" at Scuola Estiva AILA 2010, August 29 – September 4, 2010, www.ailalogica.it/attivita/scuola-aila.php

5.2 ETH Zurich: Eidgenössische Technische Hochschule Zürich, Switzerland

Partner Profile The Swiss Federal Institute of Technology Zurich (ETH Zurich, or simply ETHZ) is an institution of the Swiss Confederation dedicated to higher learning and research. ETHZ has a central infrastructure for, and considerable experience with, the administration of EU-projects; in particular, since the start of the 6th Framework Programme of the European Union, ETHZ has been involved in 178 EU projects. The Information Security Group (http://www.infsec.ethz.ch) headed by David Basin consists of more than 20 researchers, focusing on different aspects of the development of rigorous methods and tools for building secure and reliable systems, such as methods and tools for the formal specification and validation of industrial-scale security protocols, as well as the development of a framework for trust, security and contract management in dynamically-evolving virtual organizations. The group collaborates with several international academic and industrial partners. David Basin is also director of the Zurich Information Security Center (ZISC, http://www.zisc.ethz.ch), a cooperation between members of ETH Zurich and industry, with the aim of providing a coordinated program of state-of-the-art research and education in information security.

Individual Goals of Exploitation ETH Zurich has pursued two main goals in the context of AVANTSSAR: Fundamental and applied research on formal verification of security-sensitive service-oriented architectures, and using the results of AVANTSSAR for educational purposes (e.g. in the Information Security Master Track http://www.infsecmaster.ethz.ch offered by ETH Zurich). In terms of goals of future exploitation, ETH Zurich will use the results of AVANTSSAR as a basis for collaboration in national and international research projects, as well as engaging in advanced educational programs.

Identified Exploitable Project Results ETH Zurich will use the results of AVANTSSAR, in particular the AVANTSSAR Validation Platform, for educational purposes. Moreover, ETH Zurich will promote the use of the languages, techniques and tools developed in AVANTSSAR in other national and international research projects, in particular the FP7 projects SPaCIoS [20] and NESSOS [18]. For instance, the AVANTSSAR Validation Platform will provide a basis for the new technology that will be developed in the context of SPaCIoS for the validation of services at provision and consumption time.

Status Report of Exploitation Activities ETH Zurich has already exploited the project results for educational purposes in the Information Security Master Track at ETH Zurich. The results of AVANTSSAR have been our starting point for the SPaCIoS project, for which the work has already started. The challenges include a focus shift from design time to provision and consumption time: testing security-sensitive service-oriented architectures is of particular importance to SPaCIoS. ETH Zurich also will continue working on formal verification of security properties of service-oriented architectures, by extending the results obtained in the context of AVANTSSAR.

5.3 INRIA: Cassis Group, INRIA Lorraine, France

Partner Profile INRIA, the French national institute for research in computer science and control, operating under the dual authority of the Ministry of Research and the Ministry of Industry, is dedicated to fundamental and applied research in information and communication science and technology (ICST). The Institute also plays a major role in technology transfer by fostering training through research, diffusion of scientific and technical information, development, as well as providing expert advice and participating in international programs.

Individual Goals of Exploitation In participating to AVANTSSAR, we contribute to research in Security and Reliability of Computing Systems, one of the 5 scientific priorities at INRIA. New digital technologies raise numerous questions relating to security, safety and confidentiality, trust, authentication and identification, certification, data protection and traceability. The level of trust that the user has in these technologies, which include a significant software component, is key to their acceptance. INRIA commits to investigating technologies for guaranteeing that these software programs operate properly, through secure development methods (formal languages, mathematics, proof, verification, as well as software code and component certification).

Identified Exploitable Project Results INRIA plans to exploit the AVANTSSAR Validation Platform as a whole both for industry-level applications and for educational purposes at Master level. Moreover, INRIA also plans to use the languages, techniques and back-ends that comprise the platform in other national and international research projects. For instance, we will promote the use of the orchestration and security analysis technology of the AVANTSSAR Validation Platform in the FP7 project NESSOS [18].

Value Proposition

- The AVANTSSAR Orchestrator proposes a new fully automatic approach to secure service composition. This tool has strong potential for reducing time to market service design, by mitigating the complexity of security policies and messages flows.
- The AVANTSSAR validation back-end CL-AtSe offers the possibility to validate many security aspects of the (composed) services before they are released.

Value Creation We plan both to further develop CL-AtSe and the orchestrator (in cooperation with IRIT) and to apply them to a number of industrial case studies provided by the project partners but also by potential future partners. We offer both consulting, in the sense that we can apply CL-AtSe for the orchestration and validation of services developed by the potential partners, and also information exchange/training in the sense that we could offer tutorials on how to employ CL-AtSe and the AVANTSSAR technology in general to validate services and applications. We would also gladly consider external collaboration on the future development of CL-AtSe with both academic partners working on formal methods and automated reasoning for security, services and applications, and companies/industry/standardisation organizations working on service development or application.

Status Report of Exploitation Activities Both the orchestrator and CL-AtSe have been intensively tested on case-studies provided by the AVANTSSAR industrial partners. Still, the tools need to be further enhanced in order to better capture the complexity of real workflow, in particular they should handle services with richer branching and loop constructions. Moreover, for wider adoption, the tools need to be more compliant to WS standards. Therefore, we need to develop translators from standards to the AVANTSSAR specification languages and vice versa.

5.4 UPS-IRIT: LiLaC Team, Institut de Recherche en Informatique de Toulouse, France

Partner Profile The Université Paul Sabatier Toulouse 3 (UPS) is among the largest French universities dedicated to science. Its computer science laboratory, IRIT, is an institute hosting researchers from the University itself, from CNRS, and from other engineering schools in Toulouse (INPT). It is one of the main French computer science laboratories, and has been very positively evaluated in the recent years by the French AERES, both for its theoretical advances and for its partnerships with local aeronautics industry.

Individual Goals of Exploitation Security is a theme pervasive in the scientific orientations of IRIT, and is in particular in the *embedded systems* and the *Health care* research axes. Indeed, the former of these axes requires security and safety, whereas the latter requires security and privacy. The work we have done within the AVANTSSAR project fits particularly well given that both embedded systems and health care infrastructures are inherently distributed, and thus will profit, e.g., from advances on access control expression in distributed systems. In the near future, we plan to refine the results obtained on orchestration and access control by applying them on the case studies provided in the ANR Verso (Future Networks and Services) project PIMI that will start at the beginning of 2011.

Identified Exploitable Project Results We plan to reuse the theoretical results obtained in current (PIMI) and future industrial partnerships to solve case studies. In particular, we plan to continue the development of tools that will eventually integrate the AVANTSSAR Platform:

Status Report of Exploitation Activities

- We have obtained theoretical results on orchestration and equivalence validation of services.
- We are still in the process of implementing an orchestrator using the techniques that we have developed, but in the near future we plan to rely on the tools (both the TS Orchestrator and CL-AtSe) developed at INRIA when working on case studies provided by industrial partners.
- A critical point will be the availability of connectors between the WS-$\star$ standards and the ASLan language in the input and output of these tools. We plan, if necessary, to continue our collaboration with INRIA on this topic.

5.5 UGDIST: Dipartimento di Informatica Sistemistica e Telematica, Università di Genova, Italy

Partner Profile The University of Genova is one of the oldest universities in Italy with a long history of collaboration with other universities and research institutes in Europe. The Department of Communication, Computer and System Science (DIST) is the largest within the University of Genova and has a long research history in many areas of Computer Science and Computer Engineering. With around 80 members and an annual research budget of around 5.5 million euros, it is currently involved in 20 European Projects.

Individual Goals of Exploitation Software services, formal verification, software engineering and security are key areas of competence and research at UGDIST. UGDIST aims at increasing knowledge and competence on these topics for educational purposes, including the specialization of the Master and PhD students as well as of the postdoctoral researchers participating in the project. UGDIST also aims at applying the results of the AVANTSSAR Project in applied research projects with companies in the Ligurian Region.

Identified Exploitable Project Results UGDIST has developed the model checker SATMC, one of the validation back-end of the AVANTSSAR Platform and has contributed to the design of the formal specification languages developed in AVANTSSAR. Besides the results achieved in the AVANTSSAR Project, SATMC has been independently used by other researchers to develop a tool (Tookan) capable to reverse engineering PKCS#11 smartcards. By using this technology several vulnerabilities have been identified in a variety of products by Aladdin, Bull, Gemalto, RSA, and Siemens, among others. This shows that the verification technology implemented in SATMC can be already exploited in several application areas. See [22] for more details.

Status Report of Exploitation Activities UGDIST has already started exploiting the project results at the University of Genova. The techniques and tools have also been exploited by UGDIST in the context of the SINTESIS Project (www.progetto-sintesis.org/), a project of the Technological District on Integrated Intelligent Systems of the Ligurian Region, where the automated validation technologies developed in the context of AVANTSSAR have been successfully applied to validate a state-of-the-art protocol for security positioning. Work is also underway in the SPaCIoS project [20] with the ultimate goal of adapting and scaling the SATMC validation technologies to

support the automated security testing of online, distributed systems.

5.6 IBM: IBM Research GmbH, Zurich Research Laboratory (ZRL)

Partner Profile IBM Research GmbH, Zurich Research Laboratory (ZRL), with approximately 300 employees, is a wholly-owned subsidiary of the IBM Research division with headquarters at the T.J. Watson Research Center. ZRL, which was established in 1956, represents the European branch of IBM Research. It is involved in more than 80 joint projects with universities throughout Europe, in research programs established by the European Union and the Swiss government, and in co-operation agreements with research institutes of industrial partners. In the Computer Science department of ZRL, research is focused on the fields of secure and trusted systems, mobile computing, business process technology and optimization. Furthermore, the department has a long history in systems management and cryptography research. In the area of security, current research is focused on privacy and cryptography, in particular identity management, Web services and policies, intrusion detection, mobile and ubiquitous computing, and smartcards. The lab has participated in several EU-funded projects such as the PRIME project (IST-507591). Much of this research has become or had a direct influence on IBM's products and services.

IBM has withdrawn from the project on May 15, 2010, as described in the amended Description of Work and in the Deliverable D1.5 (preliminary version) Progress/Assessment Report for Year 3 of Beneficiary IBM. Still, we provide here a brief technology implementation plan for the partner.

Individual Goals of Exploitation IBM is a large software and services company with particular strengths in middleware. SOAs and web services in particular are a core area, e.g., in the IBM WebSphere brand and also as a services methodology. IBM has played a leading role in developing Web Services standards, and in particular Web Services security and policy standards and corresponding implementations. Furthermore, IBM is a provider of core security technologies, e.g., with the IBM Tivoli brand and with the IBM Internet Security Services (ISS) platform. With the increasing dynamics and configurability of these services and architectures, we perceive that tool support for the validation and ultimately verification of actually implemented or deployed versions, as enabled by the AVANTSSAR Platform, will become a must at some point in the future.

Identified Exploitable Project Results IBM Zurich Research Laboratory is the developer of the Identity Mixer protocols for providing strong authentication while protecting the privacy of the users. The Identity Mixer,

which has been used in the FP6 integrated project PRIME ("Privacy and Identity Management for Europe" [7]) and the FP7 integrated project PRIMELIFE ("Bringing sustainable privacy and identity management to future networks and services" [19]), is a complex system based on innovative cryptographic methods developed at IBM. The formalisation and validation of the Identity Mixer within the AVANTSSAR project provides a complementary view to the cryptographic proofs of the security of the Identity Mixer conducted by IBM researchers so far. The activities within the AVANTSSAR have provided a better understanding of the Identity Mixer on a more abstract level which does not focus on the cryptography, but on the interplay of all protocols and components of the system, thus contributing to the development and the quality of the system. The successful validation with AVANTSSAR will help increase the confidence into the Identity Mixer and therefore sensibly contribute to the promotion of secure privacy technologies.

Status Report of Exploitation Activities IBM has worked on the formalization of zero knowledge proofs as a cryptographic primitive, which is needed to formalize the Identity Mixer case study. In particular, we can avoid the non-trivial algebraic reasoning required by existing work, and also we can handle relations on credential attributes. This model of the Identity Mixer has been developed in cooperation with researchers at IBM that work on the PRIMELIFE project [6]. Moreover, IBM has, together with UNIVR, formalized compositional reasoning techniques based on channels, where the idea is that one has one service that provides a particular kind of channel and another service that assumes it; under certain conditions on the format of both services, we may be able to verify both services individually to be correct and use our compositionality result to infer that also their composition is correct. This in particular allows us to obtain more general verification results, which are applicable also outside AVANTSSAR: the higher application service is secure for any implementation of the lower channel service, and the lower channel service may be used for any application that requires this kind of channel. See [11, 14, 15, 16] for more details.

As another industry migration, IBM have devised the new specification languages AnB, a formal protocol description language based on Alice and Bob notation, and CARL for credential-based access control [5]. AnB improves on previous formal AnB languages by the definition of a semantics for an arbitrary algebraic theory and the notation for the aforementioned channels. AnB is integrated into the AVANTSSAR tool-chain by a translator from AnB to ASLan (for some common algebraic theories).

The language CARL has been developed in collaboration with the PrimeLife

project. The novel aspect of CARL is the ability to specify policies in a privacy-friendly way, in particular the minimum amount of information that needs to be revealed (including revealing to third parties). The language is technology neutral, however, so that established technologies (like X.509 certificates) can be used that do not necessarily ensure the level of privacy that Identity Mixer does (i.e., revealing more information than required). We have begun designing a mapping from CARL specifications to the Identity Mixer technology; this gives a new form of compositional reasoning, using the Identity Mixer protocols as building blocks of privacy-friendly service-oriented architectures.

IBM has also devised a new, general (i.e., not AVANTSSAR-specific) abstraction technique that modifies the idea of the abstraction-based approaches so that non-monotonic behavior can be modeled [12, 13]. The key idea is that participants may maintain sets of data and the abstraction interpretation of data abstracts by the set-membership of the data. IBM has also devised a variant of ASLan, called AIF, that is related to this new abstraction method.

Finally, Sebastian Mödersheim, the AVANTSSAR site leader of IBM, has moved from IBM to the Denmark's Technical University in May 2010, but he has continued to support the AVANTSSAR project. The further development of his OFMC tool in the AVANTSSAR project has been continued by the Verona partner. The AVANTSSAR platform has also been deployed in lectures at DTU.

5.7 OpenTrust

Partner Profile OpenTrust, founded in 2001, is a new leader in IT security that designs and develops next-generation software security solutions for implementing Trusted IT Ecosystems. OpenTrust provides a comprehensive set of software solutions for managing strong authentication, digital certificates, digital signature, and proof management. The principal software products of OpenTrust include:

- OpenTrust PKI: A market leader complete Public Key Infrastructure software solution for delivering and managing digital certificates.
- OpenTrust SCM: A Card Management System software solution for managing a smart card's lifecycle.
- OpenTrust SPI: A digital signature and proof management software suite.

Individual Goals of Exploitation In the context of the AVANTSSAR project, OpenTrust proposed to focus on the SPI products which are closely related to business process applications. The OpenTrust SPI suite includes different software products including SPI Security Server, which is a Web-Service-based application server used for managing digital signature operations. The SPI Security Server is used by OpenTrust's customers for implementing their business workflows involving dematerialized processes where digital signatures are needed to ensure the probative force (like digital contract signing) in replacement of handwritten signature for paper documents. In such a context, and in addition to providing the security software components (PKI infrastructure, Smart card management system and digital signature softwares), OpenTrust often provides customer service consulting for defining and fulfilling the particular security requirements related to the dematerialized processes. Thus, OpenTrust participated in the AVANTSSAR project as part of its software editor research activities in order to enrich its knowledge in formal verification of web services. Moreover, OpenTrust can benefit from the developed verification tools to formally verify our product features. Integrating this into business application design would prove to OpenTrust customers that our products fulfill their expected security requirements.

Identified Exploitable Project Results In the AVANTSSAR project, OpenTrust focus was first on the formalization of application problem cases involving document digital signing. OpenTrust worked on the DCS (digital

contract signing) and PB (public bidding) use case specifications. These use cases were specified based on real usage of OpenTrust SPI products. Some complementary steps and requirements have been added to make them more generic, so that their ASLan specifications may be easily re-used to model in the future other use cases involving digital document signature tasks. The second focus of OpenTrust in the AVANTSSAR project has been, as part of industrial dissemination, the development of a running demonstrator that can show our customers how one can formalize and validate security requirements in a business process modeler involving OpenTrust security softwares. To this end, as part of WP6, OpenTrust chose to bridge the design and deployment of business processes using an open-source framework and their formal verification using the AVANTSSAR validation tools. In this way, an application designer will be able to first design and execute a business process with web service calls to OpenTrust SPI software. This ability would allow the designer to validate the functional executability of the workflow and even obtain sample signed documents. The designer can also verify the same process modeled using the AVANTSSAR platform thanks to an automated ASLan translator specifically developed by OpenTrust. For this, the designer just needs to add security properties he wants to check in a graphical way. These features will allow the designer to validate both functional and formal aspects of its workflow without any knowledge in formal languages among the input of the AVANTSSAR verification tools like ASLan. This pre-validation ability should be of great interest just before starting the real application development step.

Value Proposition The ASLan DCS and PB specification examples would allow OpenTrust to illustrate to customers, who are potentially interested in security validation, how security requirements related to OpenTrust product features can be fulfilled and/or verified. Nonetheless, the most interesting part for OpenTrust would be the Business Process demonstrator produced in WP6. It should be valuable in OpenTrust pre-sale and consulting activities for promoting digital certificate and digital signature usage as part of a business process with critical security requirements. OpenTrust will use it for a demonstration purpose in a case to case basis should the customer expresses its interest.

Revenue Model The demonstrator is viewed as a proof of concept and OpenTrust does not intend to make a commercial product out of it since business process designing and validation is not OpenTrust core business. As thus, no direct revenue model is foreseen by OpenTrust. The gain for

OpenTrust will be indirect fallouts by considering the demonstrator as material for promoting OpenTrust products.

Status Report of Exploitation Activities The Business Process demonstrator is partly finished at the time of the writing of this document. The ASLan translation part and the web service execution extensions are functional though not terminated. There is still some development to be carried out to provide a user friendly configurator for defining security properties in the business model.

5.8 IEAT: Institute e-Austria Timişoara, Romania

Partner Profile IeAT (Institute e-Austria Timişoara) is an independent Romanian research institute for Computer Science and Information Technologies, established jointly by the "Politehnica" University and the West University of Timişoara, Romania, and the Research Institute for Symbolic Computation (RISC) Linz, Austria.

IeAT aims to concentrate computer science research in Timişoara in select fields, and to offer academic researchers from its founding partner institutions stimulating conditions to perform research in Romania rather than abroad. In particular, the institute supports early stage researchers from the two Timişoara partner universities. In addition, the institute focuses on establishing research contracts with the local industry and providing technology transfer services, with emphasis on development opportunities for SMEs. IeAT is currently involved in 6 international and 5 national research projects.

Individual Goals of Exploitation The main reason for participation in the project was to perform fundamental and applied research. Software services, formal verification, software engineering and security are key areas of competence and research at the institute. One of the main goals has been the development of methods, technologies and tools for security service validation, and strengthening the base for industrial consulting in this field. Another goal has been the education and specialization of the Master's, doctoral and postdoctoral researchers participating in the projects, and incorporating elements from the AVANTSSAR validation platform into the curriculum.

Identified Exploitable Project Results The AVANTSSAR Validation Platform can be exploited by IeAT in future research projects as well as in technology transfer with the local industry. In addition, AVANTSSAR tools can be used within Bachelor's and Master's level courses on computer security and formal verification.

Value Proposition The participation in the AVANTSSAR project has strengthened IeAT's competencies in the area of service modeling and formal validation. IeAT can develop tool support for validation (having contributed to the AVANTSSAR platform the connectors for high-level models written in ASLan++ and BPMN). The institute can also provide modeling capabilities, having worked on case studies for citizen and service portals. This expertise can be put forward in contracts with industrial companies, as well as in future research projects.

Value Creation As part of its contribution to the AVANTSSAR platform (notably the ASLan++ translator), IeAT has developed, and plans to further support, add-ons that are useful in creating and maintaining models, such as a graphical representation of workflow structure and a debugger for protocol executability. In addition, IeAT has developed techniques for detecting classes of guessing and denial-of-service attacks and will pursue their full automation within the AVANTSSAR platform.

Revenue Model As part of its focus on technology transfer to regional companies, IeAT plans to offer consulting services for modeling and validating security-oriented services using the AVANTSSAR platform. In prior years, IeAT has had contracts on software validation with a large multinational telecommunication company, which has shown recent interest in security aspects of protocols.

Status Report of Exploitation Activities IeAT will commence exploiting the AVANTSSAR project results as part of the FP7 project mOSAIC [17], where the validation activity for services developed in the project is planned to begin Spring of 2011. In addition, IeAT plans to apply to join the FP7 SPaCIoS project [20], which several project partners have started as a follow-up to AVANTSSAR. Exploitation of modeling and validation facilities in an undergraduate computer security class has been ongoing since the preparation phases of AVANTSSAR, having been met with good interest and contributing to consolidating students' understanding of attacks and defensive protocol design.

5.9 SAP: SAP AG and its SAP Research Business Unit, Germany

Partner Profile As the world's leading provider of business software, SAP delivers products and services that help accelerate business innovation for our customers. We believe that doing so will unleash growth and create significant new value — for our customers, SAP, and ultimately, entire industries and the economy at large. As one of SAP's roll-in channels for new technology, SAP Research contributes to the company product portfolio by identifying incremental and breakthrough innovation. SAP Research is highly collaborative, with a network of 13 research centers worldwide, engaging academia, technology partners, and customers in its research projects.

Individual Goals of Exploitation The overall goal of SAP research is to improve and deliver innovation to existing SAP products and contribute new items to the product portfolio to better serve our customers. AVANTSSAR contributes directly to the company strategy to achieve its objectives going into the future. The project's focus on security is part of a conscious effort to deliver not only highly functional and efficient solutions to solve our customers' business needs, but to deliver secure and robust solutions to eliminate vulnerabilities and protect against threats. As identified in Section 3, SOA, security and trust are major issues of relevance and concern for organizations in the current marketplace and will continue to be so into the future.

Since SAP is a provider of SOA solutions, the AVANTSSAR technology is directly relevant to SAP's products and as such the technology is currently being transferred to development of two different product areas, SAP Netweaver Next Generation Single Sign-On (NW-NGSSO) and SAP Netweaver BPM (NW-BPM). There is also the potential to employ the technology in other product development areas, not yet identified, in the future as new development projects begin and evolve.

Identified Exploitable Project Results All results of the project and the knowledge gained was deemed relevant to SAP's interests, now and into the future. ASLan specifications and the validation platform are particularly relevant in terms of current exploitation activities, as are the connectors that have been built for the two SAP product implementations (NW-NGSSO and NW-BPM). Further results including the toolset and TS Orchestrator have not been directly employed in the two SAP implementations, however in future there is the potential to further develop these components in new projects that have yet to be considered.

Value Proposition Formalizing and automating the validation of security and trust in SOAs has significant value to SAP and its customers. As identified in the market analysis (Section 3), security and trust is and will continue to be a critical concern for organizations across different industry domains. By formalizing and automating the process of validating their existing and new SOA systems, organizations can be more confident in their infrastructure, allowing them to focus on their core business without the costs and risks associated with security vulnerable systems, malicious attacks, data leaks and losses, system failure and inefficiencies.

Single sign-on solutions are about security on all levels of access to systems without the inconvenience of re-prompting users to enter passwords to gain access across a number of individual systems. As demonstrated by the use of AVANTSSAR to identify and allow resolution of a distinct and exploitable security vulnerability in Google's SAML-based Single Sign-on for Google Apps, vulnerabilities can be easy to overlook. A formal approach can give assurance that all vulnerabilities are identified so that they may be eliminated. Possible inclusion of this functionality in SAP's NW-NGSSO would help customers to develop robust and secure system identification and access management systems in a more efficient manner.

Complex Business Process Models can also be difficult to examine for potential security breaches without going live and exposing organizations to potential threat. Inclusion of an AVANTSSAR plugin in SAP's NW-BPM solution will allow security properties (for example, work processes such as "division of work" and data access controls) to be set and ensure their enforcement within a complex SOA model with multiple interacting components and actors involved.

Besides these two transfer projects, the technology will be available for any adaptation if required by future needs and new product developments, where relevant, to increase security and thus the quality. SAP will also be using it as a basis for further research in the new FP7 project SPaCIoS [20], of which they are a partner.

Value Creation In order to begin delivering on the value proposition described above, two internal transfer projects are being completed as part of the project's industry migration activity within WP 6 (Dissemination and industry migration). As such, two connectors/plugins have been developed to integrate the AVANTSSAR platform with the two solutions and allow transfer of data between the two. At the conclusion of the project, all relevant knowledge for these two projects will be transferred to the respective product groups so that they may be further enhanced and finalized for deployment

to customers.

In the NW-NGSSO industry migration initiative, SAP have exploited the AVANTSSAR technology to formally analyze SAP-relevant scenarios where the SAML-based NW-NGSSO services are employed. During the analysis more than 50 formal specifications were written, capturing these scenarios, the variety of configuration options, and the SAP internal design and implementation choices. The analysis conducted with AVANTSSAR shows that the SAP NW NG SSO services are indeed well designed. Safe and unsafe service compositions and configurations have been identified, so that the safe ones can be used by SAP in setting-up the NW NGSSO services on customer production systems. The next step in this case could be to automate the process of generating formal specifications to make the process less labour intensive and complex. Such activity is not yet a necessity, but nonetheless can be considered at a later date.

For SAP NW-BPM, an eclipse plug-in extension was developed to enable a business process modeler to specify security goals, for example "division of work" and data access controls. The plug-in is then able to perform security validation of models to ensure accurate implementation of the intended security goals.

Revenue Model At this stage, while the technology has been transferred to two development divisions it has not yet been produced. The decision of whether to release such functionality will be made at a later stage, once the development division has been able to assess the feasibility of including such functionality and the degree to which the technology can be integrated with the existing solution. Furthermore, if successfully released, the revenue that may be attributed to AVANTSSAR is difficult to quantify as it is being used as one piece of functionality within each overall solution, rather than as a product in its own right. In the future, thanks to the unique and expert knowledge built up during the project, there may be an opportunity for revenue through a consultation service model, to adapt the AVANTSSAR platform and other components to a new instance to serve a customer directly. This option, however, is unlikely to be explored in the near future and therefore cannot be further expanded upon here. There is also future potential to offer AVANTSSAR functionality as part of an on demand platform, in conjunction with other SAP software. In this case, AVANTSSAR could generate a service revenue scheme. Again, the feasibility of such an offering is not yet attractive enough to warrant investment, but as the technology matures through new research projects, this may change in the future.

Status Report of Exploitation Activities As the project rapidly approaches completion and closure, significant success has been reached with regard to the intended outcomes and exploitation of the project. The following points summarize the status and future directions for the outcomes of the project:

- Successful meeting with the SAP NW-BPM group, who were very satisfied with the research results.
  - The prototype has been optimized and scalability issues have been address to significantly improve performance.
  - The next step is for the prototype to begin the production processes within the NW-BPM team.
- SAP NW-NGSSO now has over 50 specifications of possible implementations (generated manually) that safely adhere to security and trust protocols.
  - In the future, there is potential to automate the specification process to make it more attractive to customers with diverse system and security requirements.
- Dissemination through various internal communication channels to share the results of the project with SAP's global research community and provide the potential for further transfer projects to be identified in the future. These may include publishing of articles in SAP Research Insights, SAP Developer Network and other internal publications.
- Knowledge transfer to the research project SPaCIoS [20], of which SAP is a partner.
- Further dissemination activities include: journal or conference papers, support of other project partners, approaching standardization bodies in an effort towards establishing the technology and AVANTSSAR as a de facto standard for automated validation of security and trust of SOAs.
  - This could potentially provide opportunities for consultation by SAP or other project partners to deploy the technology for an individual customer project.

5.10 SIEMENS: Siemens Aktiengesellschaft, Corporate Technology, Security, Germany

Partner Profile Siemens AG is a global powerhouse in electronics and electrical engineering, operating in the industry (including transportation), energy, and health sectors. Siemens holds leading market positions in all its business areas, working to develop and manufacture products, design and install complex systems and projects, and tailor a wide range of solutions for individual requirements. For over 160 years, Siemens has stood for technological excellence, innovation, quality, reliability and internationality. In the fiscal year 2009, Siemens had revenue of 76.7 billion Euros. Today the company employs around 17.000 software engineers and researchers with a strong expertise in software development. The degree of innovation and the market success is significantly driven by software being an inherent element of most of our products. This makes Siemens one of the world's largest software houses.

Individual Goals of Exploitation Today, SIEMENS is working on the design and development of IT Solutions for infrastructure control, automation, industrial production, medical equipment, Health Telematics Infrastructure, Patient Data Analysis, Power transmission systems on electrical grids (including negotiation), power generation and others.[4]

In all those examples, and also in future and potential SIEMENS developments, secure inter-working is absolutely necessary to avoid tampering of critical data leakage of information to untrusted parties. A particular aspect of these examples is the dynamic character of the communication relations, trust assumptions, security requirements, and even of the business relations.

Value Proposition The AVANTSSAR results are crucial to tackle the challenge of offering secure dynamically composed services in a verifiable way that increases the competitive edge of the products of SIEMENS, raises and sustains the trust of customers and partners in the complex applications built by the company, and proves to be adequate for Common Criteria certification at higher assurance levels.

[4]At project proposal time and during part of the AVANTSSAR lifetime, Siemens IT Solutions and Services (SIS) was working additionally on tools for Software Distribution Services and on E-Government (concretely, Citizen Portals and Document Exchange Procedures), but those activities have remained at SIS which has been carved out and will be sold to Atos Origin, making Atos the fifth largest IT services company in the world, and the second largest in Europe, after IBM.

The most important result of Siemens is ASLan++ as a means to formally specify the security aspects of complex and dynamic services of all kinds, in a style well accessible to software engineers because modeling in ASLan++ feels much like programming in contemporary high-level programming languages. This will play an important role in particular in the design phase of new products, but also in the security analysis of already existing products. The specification language has already proved as a very suitable instrument for pinning down in a both concise and complete way the most relevant security mechanisms and security goals of a system. It thus helps enormously in designing and documenting security services, and finding potential security loopholes already at design stage when it is by far most cost-effective.

Moreover, the AVANTSSAR tools, including the ASLan++ Connector and the various model-checking back-ends, play a crucial role in validating the correctness of an ICT system's security architecture and its ASLan++ model. They give the modeler precious feedback on the quality of the model.

Status Report of Exploitation Activities The practical applicability and value of the AVANTSSAR language and toolset have already been proven in the (formerly) Siemens SIS realm, where two colleagues without formal modeling background produced and verified security models of a SPOCS [21] citizen portal application scenario and of a business-critical intranet service platform. They have been able to do this with comparatively little effort and still very useful results, mostly in the form of feedback to the design, implementation, and documentation teams. Similar success stories are expected for other business units and their products.

A further strong line of exploitation is expected in the FP7 project SPaCIoS [20], where the aim of Siemens and its partners is to perform security testing with formal techniques, which will most likely be based on ASLan++ and the related tools. Also the newly started ITEA2 project DIAMONDS [8], to which Siemens will be associated, is likely to directly benefit from the AVANTSSAR results.

References

[1] AVANTSSAR. Deliverable 6.2.1: State-of-the-art on specification languages for service-oriented architectures. Available at http://www.avantssar.eu, 2008.

[2] AVANTSSAR. Deliverable 1.6: Final Dissemination and Use Plan. Available at http://www.avantssar.eu, 2010.

[3] AVANTSSAR. Deliverable 5.3: AVANTSSAR Library of validated problem cases. Available at http://www.avantssar.eu, 2010.

[4] AVANTSSAR. Deliverable 6.3: Migration to standardisation bodies. Available at http://www.avantssar.eu, 2010.

[5] J. Camenisch, S. Mödersheim, G. Neven, F.-S. Preiss, and D. Sommer. A Credential-Based Access Control Requirements Language. In *SACMAT'10*. ACM Press, 2010.

[6] J. Camenisch, S. Mödersheim, and D. Sommer. A formal model of identity mixer. In *FMICS'10*, LNCS 6371. Springer, 2010.

[7] J. Camenisch, A. Shelat, D. Sommer, S. Fischer-Hübner, M. Hansen, H. Krasemann, G. Lacoste, R. Leenes, and J. Tseng. Privacy and identity management for everyone. In *ACM DIM*, 2005.

[8] DIAMONDS. www.fokus.fraunhofer.de/en/motion/projekte/laufende_projekte/DIAMONDS.

[9] 2010 Update: What Organizations Are Spending on IT Security. www.gartner.com, 2010.

[10] Key Issues for Information Security, 2010. www.gartner.com, 2010.

[11] T. Gross and S. Mödersheim. Vertical Composition of Protocols. submitted, 2010.

[12] S. Mödersheim. Abstraction by Set-Membership—Verifying Security Protocols and Web Services with Databases. In *17th ACM Conference on Computer and Communications Security (CCS 2010)*, 2010.

[13] S. Mödersheim and P. Modesti. Verifying SeVeCom Using Set-based Abstraction. Imm-technical report-2011-01, DTU Informatics, Denmark, 2010.

[14] S. Mödersheim and L. Viganò. Secure Pseudonymous Channels. In *Proceedings of Esorics'09*, LNCS 5789, pages 337–354. Springer-Verlag, 2009.

[15] S. Mödersheim and L. Viganò. The Open-source Fixed-point Model Checker for Symbolic Analysis of Security Protocols. In *Fosad 2007-2008-2009*, LNCS 5705, pages 166–194. Springer-Verlag, 2009.

[16] S. Mödersheim and L. Viganò. Channels as Assumptions, Channels as Goals, 2010. Submitted journal paper.

[17] mOSAIC: Open-Source API and Platform for Multiple Clouds. www.mosaic-cloud.eu.

[18] NESSOS: Network of Excellence on Engineering Secure Future Internet Software Services and Systems. www.nessos-project.eu, 2010.

[19] PrimeLife: Bringing sustainable privacy and identity management to future networks and services. www.primelife.eu.

[20] SPaCIoS: Secure Provision and Consumption in the Internet of Services. spacios.eu, 2010.

[21] SPOCS: Simple Procedures Online for Cross-border Services. eu-spocs.eu, 2009.

[22] Tookan: TOOl for cryptoKi ANalysis. http://secgroup.ext.dsi.unive.it/projects/security-apis/pkcs11-security/tookan/.

[23] Security holes in PayPal's iPhone app. http://www.zdnet.com/blog/security/security-holes-in-paypals-iphone-app/7670, 2010.

[24] Technical Standard. http://en.wikipedia.org/wiki/Technical_standard, 2010.