Research and Innovation Yearbook 2013

Fabio Massacci, Olga Gadyatskaya (University of Trento)
Nick Wainwright (Hewlett-Packard Limited)
Paul Malone (Waterford Institute of Technology)

Version 1.2 September 2013

Executive Summary

The aim of this Yearbook is to investigate the R&D projects executed under the Trust & Security Programme and present the discoveries of the study conducted with the project leaders. The Yearbook has also an objective to serve as a reference for the Trust & Security Programme projects: what are the key innovative results produced by the projects, how do the projects handle market acceptance gaps for their technologies, and where to find more details regarding a certain project. In contrast to the CORDIS system [1], where the project descriptions sometimes are vague because they are taken directly from project proposals, this Yearbook presents key details of project R&D innovation achievements shared by projects' leaders.

For the scope of the Yearbook we group the projects according to their state: projects launched in Call 1 and the Joint ICT-SEC Call have completed several years ago; projects executed in Call 5 and the ICT-FI Call have either completed their activities in the last year or are in the completion phase; and projects selected in Call 8 have started in the last year. During our study we have contacted projects of the Trust & Security Programme, requesting to share some details of the projects' activities, such as publishable summaries of completed projects; publication lists, dissemination and exploitation strategies and project presentations for active projects. For the projects in Call 5 and Call 8 we have also asked for an interview with project leaders to gain more insight about project activities. However, not all contacted projects have replied to us. Therefore the Yearbook contents are divided into two parts:

- *Analysis of the Trust & Security Programme projects as a whole* with respect to addressing the Work programmes' objectives, key domains for the projects' results applications, the participants landscape and potential contributions of the Programme to the NIS Platform initiative. We also report notable findings from the interviews with the project leaders regarding the status of the EU ICT Security Domain.
- *Reference guide for the interviewed Trust & Security Programme projects* with key innovation achievements, market acceptance gaps and interesting details of what is going on in the project. This reference guide is based on a series of interviews UNITN has conducted with coordinators and participants of the presented projects.

Summary of the Trust & Security Programme Analysis

The Programmes' goals (as defined in the Work Programmes) were mostly addressed by the selected projects. The only sub-objective of the Work Programmes that was consistently not targeted by the selected projects regards coordination with the national and regional research programmes (of the Member States).

The EU Trust & Security projects are in a good position to contribute to the NIS Platform initiative proposed recently by the European Commission as an instrument to improve the EU cybersecurity status. In the Yearbook we list the projects that have gained expertise and developed technologies in the domains currently required by the NIS Platform: risk management and security awareness promotion in organizations; threats information exchange across organizations; and roadmapping for secure ICT research and innovation.

The EU R&D projects produce results that are used in a variety of industry sectors, not only ICT Security: Critical Infrastructures and Emergency Handling; Energy and Utility; Software and IT Services; Healthcare; Telecommunications; Public Administration; Internet Services; and others. Players from these domains participate in the projects as validation experts and are ready to adopt the delivered technologies.

The interviewed project participants have shared their opinions on the status of the EU ICT Security domain. The interviewees have reported on the gap in the industrial acceptance of the technologies delivered by research projects, and have suggested to address it with validation and exploitation-oriented small-scale projects and by putting more efforts into market analysis and technology maturity. Also the skills gap in the EU ICT Security domain was noted, and the lack of security awareness in citizens as well as employees. It is remarkable that the opinions of the project leaders

are completely inline with the goals of the NIS Platform and the recent Proposal for the new EU Cybersecurity Directive.

We would like to thank all project representatives that have participated in our study.

This work has been funded by the European Commission under the FP7 SecCord Project N° 316622 (http://www.seccord.eu). The Yearbook document is an extract from the SecCord Deliverable D3.1 "Research and Innovation Yearbook".

TABLE OF CONTENTS

List of Figures

List of Tables

Abbreviations

BYOD	Bring Your Own Device
CI	Critical Infrastructure
CSP EU FORUM	Cyber Security & Privacy Forum
EFFECTS+	European Framework for Future Internet – Compliance, Trust, Security and Privacy through effective clustering
NIS PPP	Network and Information Security Public-Private Platform
SecCord or **SECCORD**	SECurity and trust COoRDination and enhanced collaboration
SIEM	Security Information and Event Management
SOA	Service-Oriented Architecture

Outline of the Trust & Security Programme

The Trust & Security Programme is a part of the 7th Framework Programme for Research and Technological Development in Information and Communication Technologies (FP7-ICT). It has comprised several Calls for R&D projects in Trust & Security[1]. So far **82** R&D projects were launched according to the CORDIS system [1]. Among those, **33** projects were executed in Call 1 (for the scope of this Yearbook we include the Joint ICT-SEC Call projects in Call 1); **28** projects were launched in Call 5 (for the scope of the Yearbook we include the ICT-FI Call in Call 5); and **21** projects have started in 2012, selected in Call 8. At the moment of writing this Yearbook the projects selected in Call 10 were not yet published in the CORDIS system; therefore we do not include these projects in the study.

Main Objectives of the Calls

Call 1 and the Joint Call between ICT and Security Themes on Critical Infrastructure Protection under Work Programme 2007-2008

The main objectives of Work Programme 2007-2008 regarding these Calls were: *Objective ICT-2007.1.4: Secure, dependable and trusted Infrastructures* and *Objective ICT-SEC-2007.1.7: Critical Infrastructure Protection*.
The following target outcomes were identified in the Work Programme for these two objectives (for the Objective ICT-SEC-2007-1.7 the focus of the ICT Theme is applicable):

- Security and resilience in network infrastructures
- Security and trust in dynamic and reconfigurable service architectures
- Trusted computing infrastructures
- Identity management and privacy enhancement tools
- Longer term visions and research roadmaps: metrics and benchmarks for technology evaluation in support of certification and standardization, international cooperation and coordination
- Technology building blocks for creating, monitoring and managing critical information infrastructures, including longer term visions and research roadmaps

Call 5 under Work Programme 2009-2010 and Call ICT-FI under Work Programme 2011-2012

The main objective of Work Programme 2009-2010 regarding Call 5 was *Objective ICT-2009.1.4: Trustworthy ICT*.
The target outcomes for the Call 5 projects:

- Trustworthy network infrastructures
- Trustworthy service infrastructures
- Technology and tools for trustworthy ICT
- Networking, coordination and support

Call ICT-FI was active under Work Programme 2011-2012. However, the projects executed under this call so far (ENVIROFI, INSTANT MOBILITY and SAFECITY) have already concluded their activities. As we investigate different aspects of projects depending on their status, we group the ICT-FI projects with Call 5, because they have all completed in 2013, what aligns with the timeline of Call 5. The main objective of Work Programme 2011-2012 regarding the Future Internet Public-Private Platform was *Objective FI.ICT-2011.1.8 Use case scenarios and early trials.*
The following target outcomes were set:

- Characterization of vertical use case scenarios for innovative applications making use of advanced Future Internet capabilities; specification of platform requirements; development of prototypes and large scale experimentation and validation.

Call 8 under Work Programme 2011-2012

Work Programme 2011-2012 defined for the Call 8 projects *Objective ICT-2011.1.4: Trustworthy ICT*.

[1] http://cordis.europa.eu/fp7/ict/security/fp7-calls-trustworthy_en.html

The target outcomes for Call 8:

- Heterogeneous networked, service and computing environments
- Trust, eIdentity and Privacy management infrastructures
- Data policy, governance and socio-economic ecosystems
- Networking and Coordination activities

Target Outcomes and Corresponding Projects Categories in CORDIS

The CORDIS system classifies the FP7-ICT projects in Trust & Security into several categories as represented in Figure 1 [1]. Categories identified in this figure are mapped into the target objectives of the Work Programmes in Table 1. Notice that this is a rough mapping, as most of the objectives' descriptions allow for more than one category; we present only those that have projects selected in the corresponding Calls.

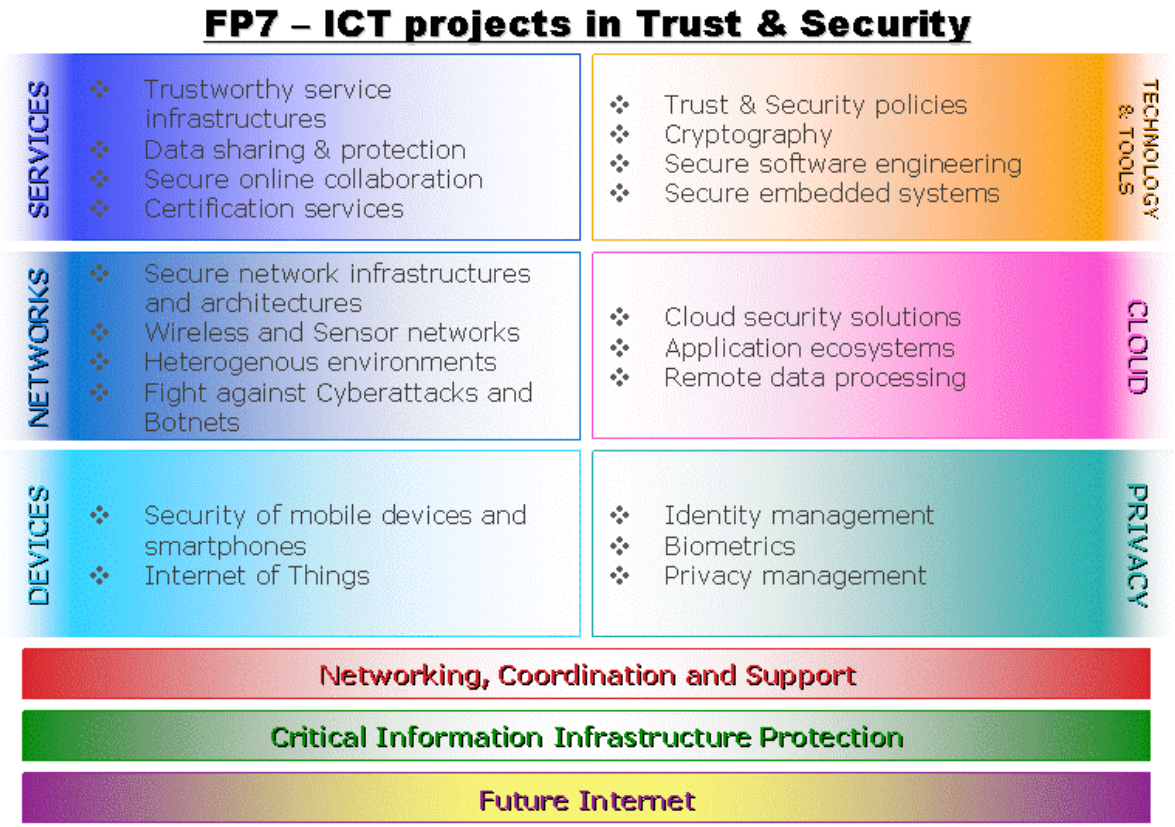

Figure 1. FP7-ICT projects in Trust and Security (from CORDIS [1])

Notice that some projects execute across the categories presented in Figure 1. For example, the TRESSCA project form Call 8 contributes to both the Cloud Security category and the Mobile Devices and Smartphones category; the ACDC project from Call 8 spans across Trustworthy Network Infrastructures, Mobile Devices and Smartphones, and Technology&Tools.

Table 1. Objectives of the Calls and corresponding CORDIS categories

Objective	Category
Call 1	
ICT-2007.1.4: Security and resilience in network infrastructures	Trustworthy Network Infrastructures
ICT-2007.1.4: Security and trust in dynamic and reconfigurable service architectures	Trustworthy Service Infrastructures
ICT-2007.1.4: Trusted computing infrastructures	Technology&Tools, Trustworthy Service Infrastructures
ICT-2007.1.4: Identity management and privacy enhancing tools	Privacy Management
ICT-2007.1.4: Longer term visions and research roadmaps	Networking, Coordination and Support
ICT-SEC-2007.1.7-Focus ICT: Technology building blocks for creating, monitoring and managing critical information infrastructures, including longer term visions and research roadmaps	Critical Information Infrastructure Protection
Call 5	
ICT-2009.1.4: Trustworthy network infrastructures	Trustworthy Network Infrastructures, Cloud Security
ICT-2009.1.4: Trustworthy service infrastructures	Trustworthy Service Infrastructures, Privacy Management
ICT-2009.1.4: Technology and tools for trustworthy ICT	Technology & Tools, Mobile Devices and Smartphones
ICT-2009.1.4: Networking, coordination and support	Networking, Coordination and Support, Future Internet
FI.ICT-2011.1.8 Use Case Scenarios and early trials	Future Internet
Call 8	
ICT-2011.1.4: Heterogeneous networked, service and computing environments	Trustworthy Network Infrastructures, Future Internet, Technology&Tools, Cloud Security, Mobile Devices and Smartphones
ICT-2011.1.4: Trust, e-identity and privacy management infrastructures	Trustworthy Service Infrastructures, Privacy Management
ICT-2011.1.4: Data policy, governance and socio-economic ecosystems	Cloud Security, Technology&Tools
ICT-2011.1.4: Networking and coordination activities	Networking, Coordination and Support

Funding Distribution

Figure 2 presents the breakdown of funding contributed by the European Commission for projects (in all Calls considered) that appear in the corresponding category in CORDIS [1]. Notice that the projects that span across categories were attributed to all categories for this chart. From this figure we can conclude that projects from the categories Trustworthy Service Infrastructures and Technology&Tools have acquired the most funding across the three Calls (21%). Privacy

Management and Trustworthy Network Infrastructures also have received significant funding (14%). Less funded are Critical Information Infrastructure Protection and Cloud Security (both have received 7% of funds); Future Internet (6%); Mobile Devices and Smartphones (5%); and Networking, Coordination and Support (5%).

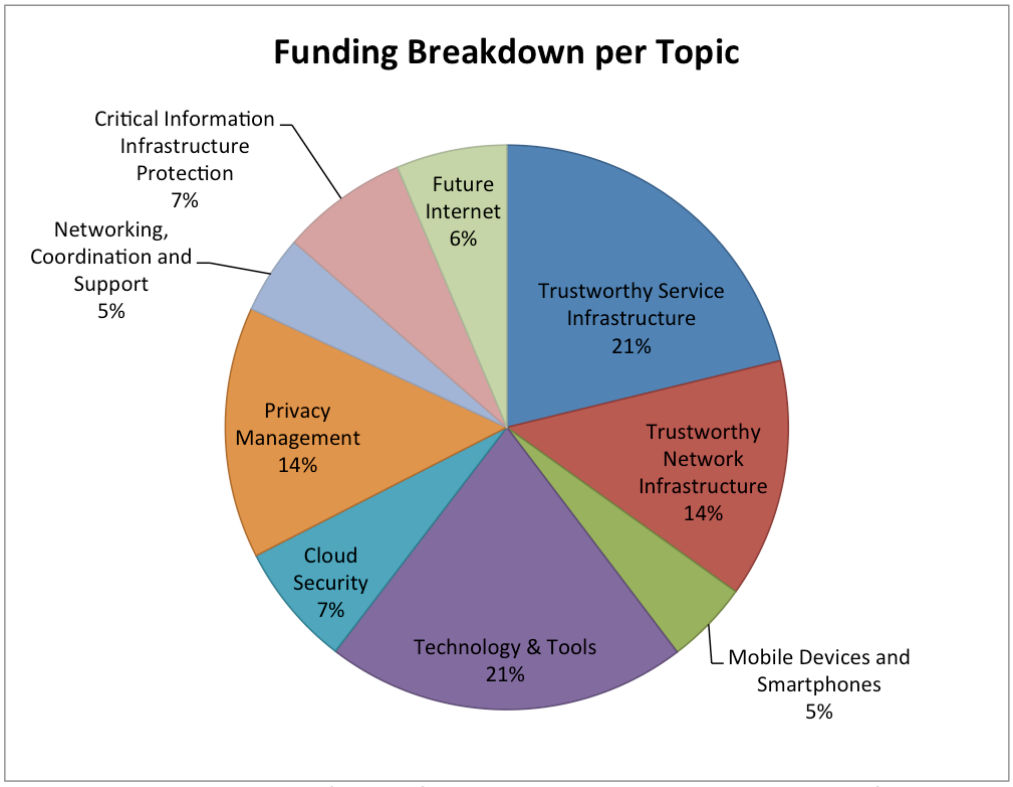

Figure 2. Funding from EC breakdown per category, across Calls

Funding distribution per Call is presented in Figure 3. We can see that Call 1 (with the Joint ICT-SEC Call) has received the biggest share (37%); but the difference between Call 1 and Call 8 with the least funding (29%) is not that significant. We can also recall that Call 8 has the least number of projects. In fact, the chart in Figure 4 shows that (on average) the projects selected in Call 8 are the best funded.

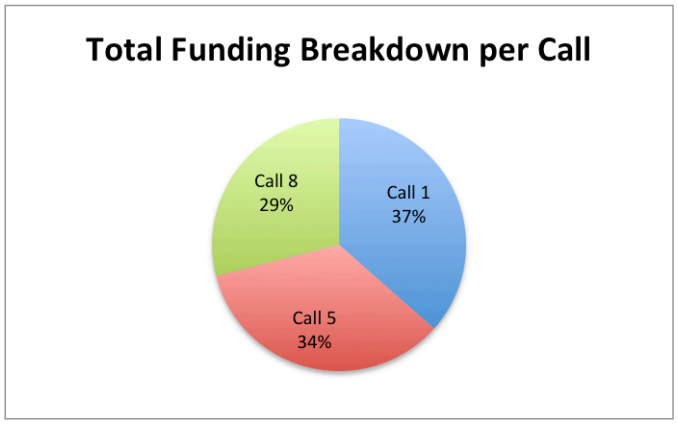

Figure 3. The EC Funding per Call

Figure 5 contains the box-plot diagrams of the project funding distribution in each Call. We can see that while the median, the first quartile, min and max statistics of the received funding in each Call are almost the same, indeed the Call 8 projects tend to be funded better.

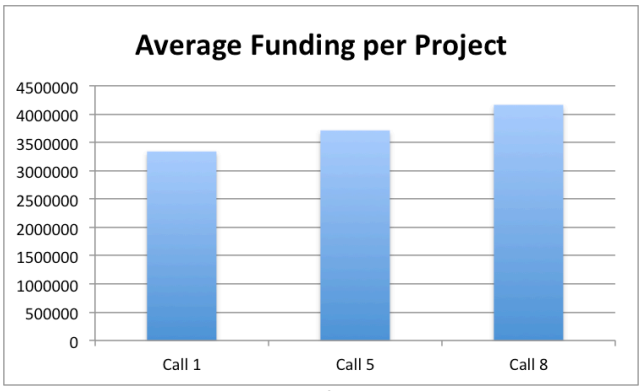

Figure 4. Average funding per project

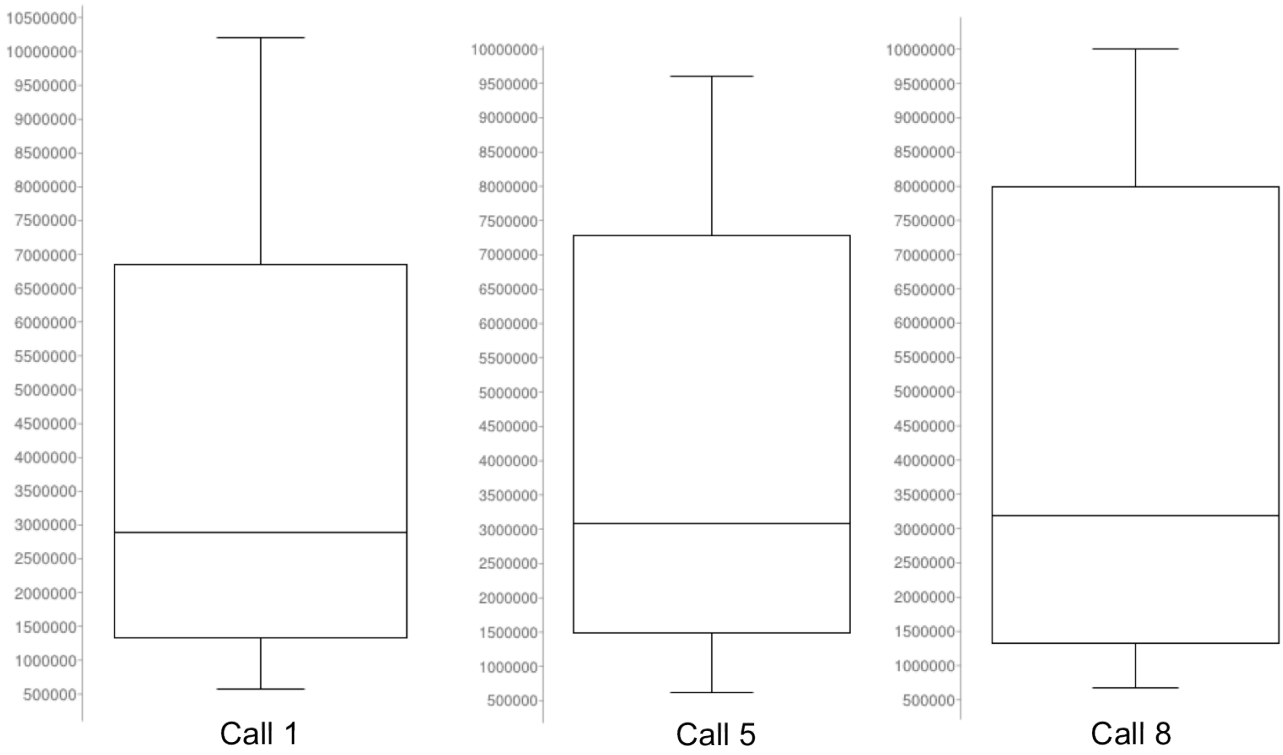

Figure 5. Box-plot diagrams of project funding distribution

Finally, Figure 6 and Figure 7 present how the funding of projects from the CORDIS project categories has evolved across Calls. We can notice that the Trustworthy Network Infrastructures category was supported almost equally throughout the Calls. Call 1 had more emphasis on privacy management and critical infrastructures protection. Such categories as Mobile devices and Smartphones, Cloud Security and Future Internet received no funding in Call 1.
Call 5 has received the most funding for the Trustworthy Service Infrastructures and Future Internet categories. And the projects from Call 8 have the biggest shares in Networking, Coordination and Support; Mobile Devices and Smartphones; Technology&Tools and Cloud Security.

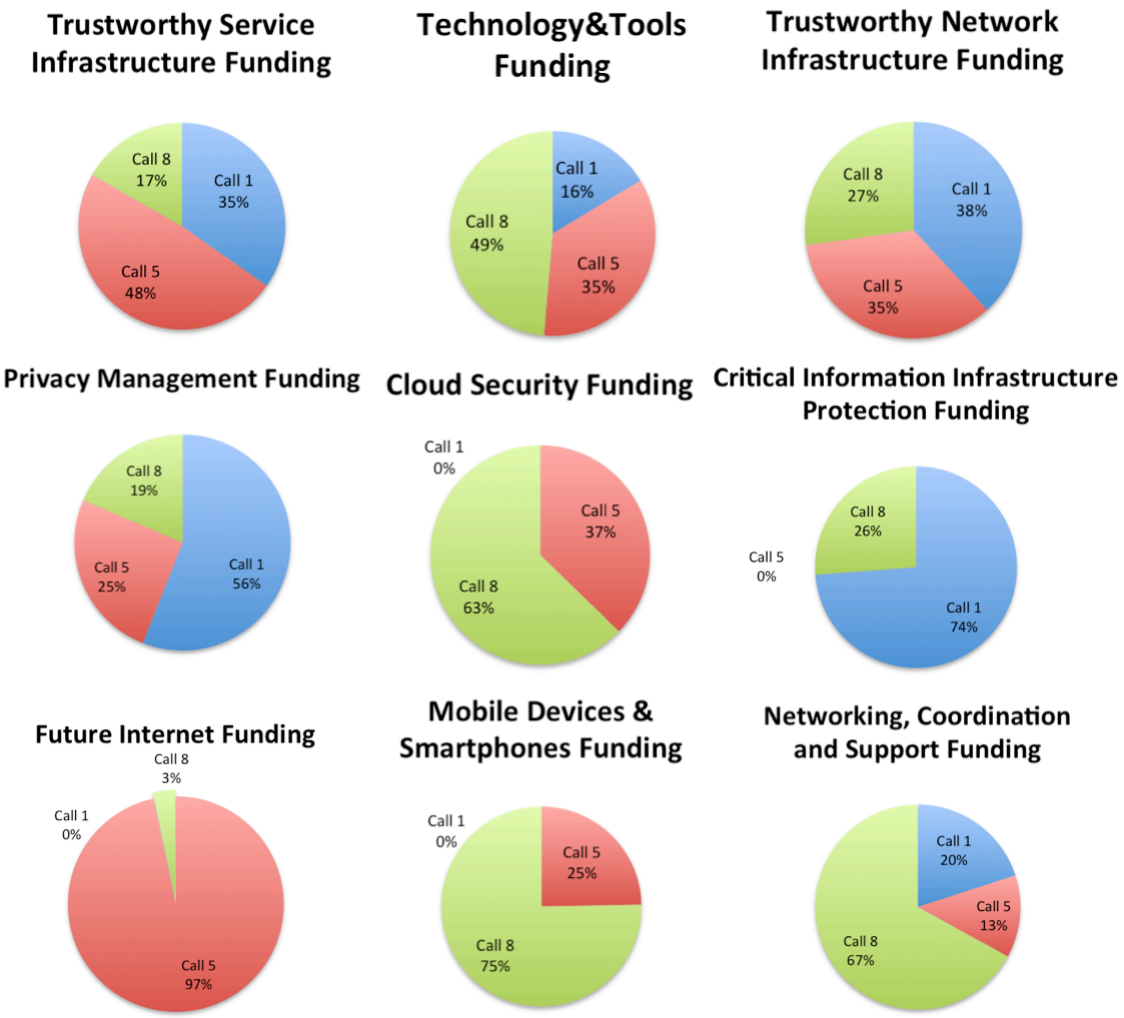

Figure 6. Funding per topic, distributed per Call

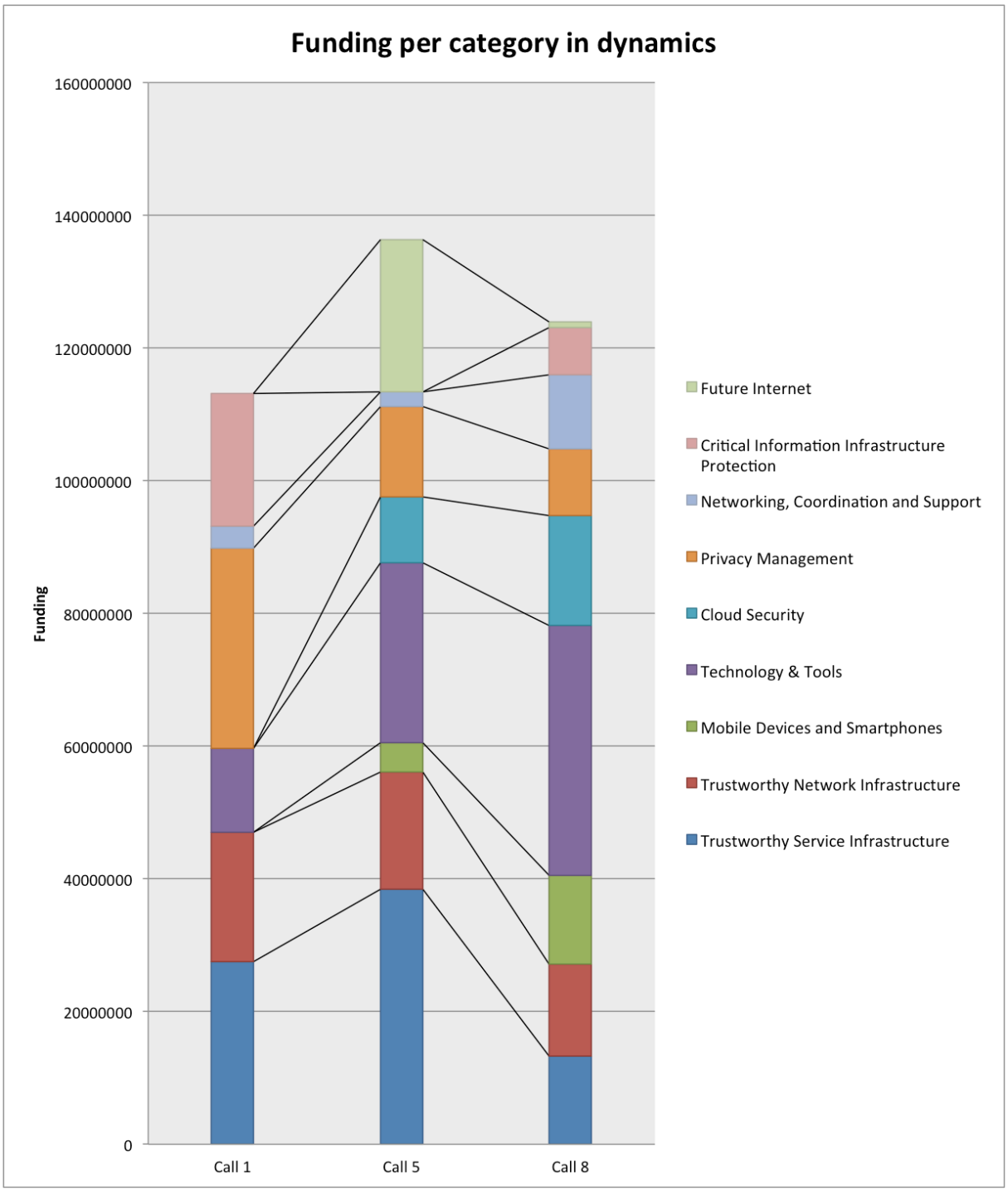

Figure 7. Funding per topic in each Call, in dynamics

Keywords for R&D Projects

We now present the keywords for the Trust & Security Programme Projects. We have identified these keywords to ease looking up projects contributing to a specific domain which does not necessarily coincide with those identified by the CORDIS categories: e.g. *cybersecurity* spans across several categories; *coordination* belongs to only one category, and *biometrics* is a subset of a single category.

Table 2. Keywords for the R&D projects in Trust & Security

Keyword	Call 1	Call 5	Call 8
Authentication	ACTIBIO, MOBIO, SWIFT	ABC4TRUST	
Biometrics	ACTIBIO, MOBIO, TURBINE	TABULARASA	
Certification	SHIELDS	ASSERT4SOA, SEPIA	EURO-MILS, D-MILS
Cloud security		TCLOUDS	A4CLOUD, TRESCCA, CIRRUS, CUMULUS
Coordination and *Roadmapping*	INCO-TRUST, PARSIFAL, THINKTRUST, ECRYPTII	SYSSEC, BIC, EFFECTS+, NESSOS	CYSPA, SECCORD, OPTET, ACDC, FIRE, STREWS, CIRRUS
Critical Infrastructure	MICIE, UAN, VIKING, COMIFIN, INSPIRE, PARSIFAL, PEACE, SERSCIS	MASSIF	
Cryptography	CACE, ECRYPTII	TAMPRES	
Cybersecurity	VIKING, AWISSNET, FORWARD, INSPIRE, INTERSECTION, PRISM, WOMBAT	DEMONS, VIS-SENSE	ACDC, CYSPA
Data sharing	CONSEQUENCE, SECURESCM		
Distributed policy	CONSEQUENCE, SECURESCM, TAS3	SPACIOUS, WEBSAND	
Economics in security		ENVIROFI	
Embedded systems	TECOM, WSAN4CIP	TAMPRES, SECFUTUR	EURO-MILS, D-MILS, HINT
Event analysis	MICIE, COMIFIN, WOMBAT	MASSIF	
Finance	COMIFIN, PARSIFAL		
Future Internet		INSTANT MOBILITY, NESSOS, SAFE CITY	STREWS
Governance, Risk and Compliance	MASTER	ENDORSE	A4CLOUD
Hardware security	CACE, TECOM, WSAN4CIP	TAMPRES, SECFUTUR, SEPIA	HINT
Identity management	PICOS, SWIFT, TURBINE	ABC4TRUST, GINI-SA	FUTUREID
Intrusion detection	VIKING, AWISSNET		
Legal aspects		ENDORSE, GINI-SA, TCLOUDS	RASEN, MUSES
Malware	FORWARD	SYSSEC	NEMESYS
Mobile security	MOBIO	SEPIA, UTRUSTIT, SYSSEC	MUSES, NEMESYS, ACDC
Negotiation	CONSEQUENCE		
Network security	AWISSNET, COMIFIN, GEMOM, INSPIRE, INTERSECTION, PRISM,	DEMONS, PINCETTE, VIS-SENSE	ACDC, D-MILS

Keyword	Call 1	Call 5	Call 8
	PEACE		
Organizational policies and *Organizational security*	CONSEQUENCE, MASTER	ANIKETOS, MASSIF, POSECCO, ENDORSE	MUSES
Privacy	PICOS, PRIMELIFE, PRISM, SWIFT, TAS3, TURBINE	ABC4TRUST, GINI-SA, TCLOUDS, TWISNET	FUTUREID, MUSES
Resiliency	AMBER, INTERSECTION, SERSCIS, GEMOM, INSPIRE, INTERSECTION	TCLOUDS	
Risk assessment and *Risk prediction*	MICIE, MASTER		RASEN, TRESPASS
SCADA	VIKING, MICIE		
Security testing		SPACIOUS	RASEN
Self-adaptive systems	SERSCIS, GEMOM		MUSES
Sensitive data management and processing	TAS3		TRESCCA
Service security	AVANTSSAR	ANIKETOS, ASSERT4SOA, MASSIF, NESSOS, SPACIOUS, WEBSAND	CUMULUS
SIEM		MASSIF	
Smart cities		SAFE CITY	
SOA security	AVANTSSAR, SERSCIS	ANIKETOS, ASSERT4SOA, SPACIOUS	INTER-TRUST, ATTPS, OPTET, CUMULUS
Social and socio-technical aspects		ENVIROFI	TRESPASS
Social networks	PICOS, PRIMELIFE		
Software security	AMBER, CACE, SHIELDS	SYSSEC, NESSOS	STANCE
Standardization	INSPIRE, INTERSECTION		
Supply chain management	SECURESCM		
Traceability	MASTER	POSECCO	
Traffic analysis	AWISSNET	DEMONS	
Transport		INSTANT MOBILITY	
Trust and Trustworthiness	AVANTSSAR, THINKTRUST	ANIKETOS, ACTOR, BIC, UTRUSTIT	ATTPS, FIRE, OPTET, CYSPA, INTER-TRUST
Usability		UTRUSTIT	MUSES, FUTUREID
Virtualization		SEPIA	EURO-MILS, D-MILS, TRESCCA
Vulnerabilities and *Vulnerabilities*	SHIELDS, WOMBAT	DEMONS, VIS-SENSE	NEMESYS, ACDC

Keyword	Call 1	Call 5	Call 8
Repository			
Web security	WOMBAT	ENVIROFI, WEBSAND	STREWS
Wireless sensor networks security	AWISSNET, GEMOM, WSAN4CIP	TAMPRES, TWISNET	

Participants Landscape

Participants Profiles

454 organizations have participated in the three Trust & Security Programme Calls; including 234 private industry organizations, and 220 research and non-commercial organizations. Figure 8 breaks down the project participants into the following categories: research centres, universities, private industry organizations, practitioners alliances, standardization or regulation body, local authorities (communes), and other types of organizations. We can see that private industry organizations represent almost half of the participants community. Research organizations are also significantly represented.
Notice that for the scope of this subsection private industries category in the figures does not include alliances of practitioners and standardization and regulation bodies with a clear commercial orientation, as they are categorized separately. In contrast, the next subsection dedicated to profiling the industry participants includes only organizations of these types that are commercially oriented. To exemplify the distinction: for the scope of this study the Belgian EEMA e-identity experts alliance (a commercial organization with paid membership) is included in the private industry category, while the Belgian LSEC alliance of security experts is a nonprofit organization. The category "other" corresponds to nonprofit organizations that cannot be classified in any other category, e.g. small educational centres.

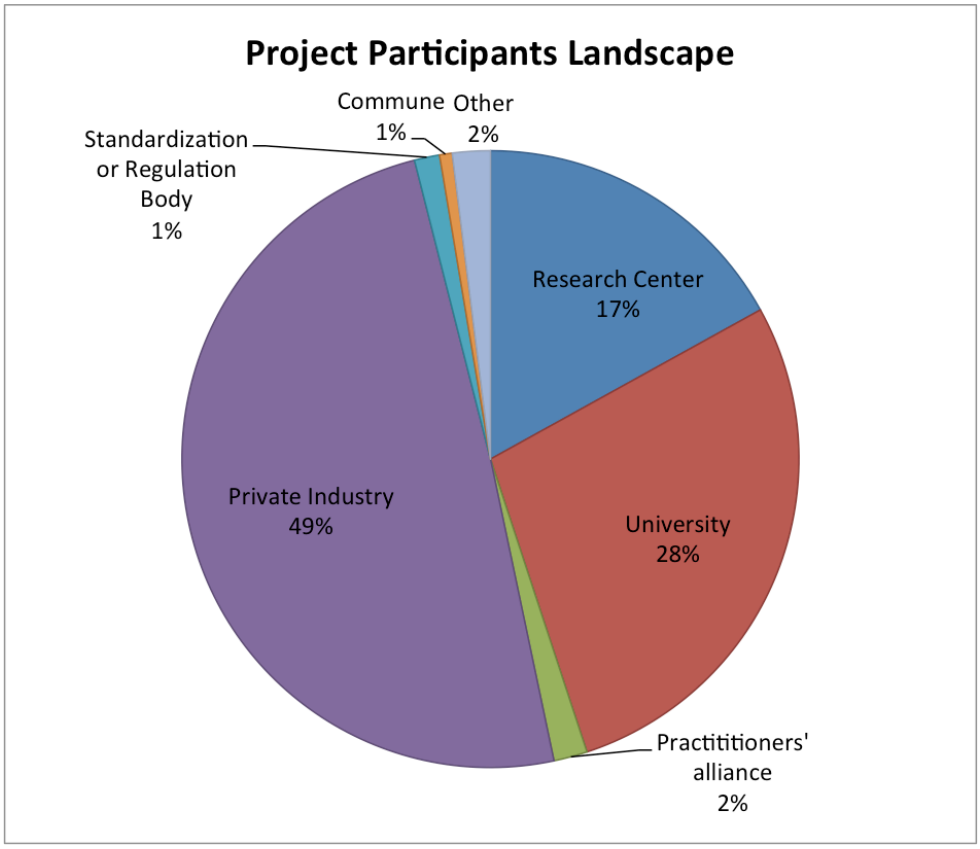

Figure 8. Breakdown of project participants across Calls

Figure 9 presents the participants shares in Call 1, which in total had enjoyed 228 participating organizations, out of which 101 were private industry organizations. From the Figure it is clear that Call 1 has attracted more universities than other Calls (28% and 27% respectively in Call 5 and Call 8), while the research centres participation agrees with average across Calls. Communes and practitioners alliances did not participate in Call 1.

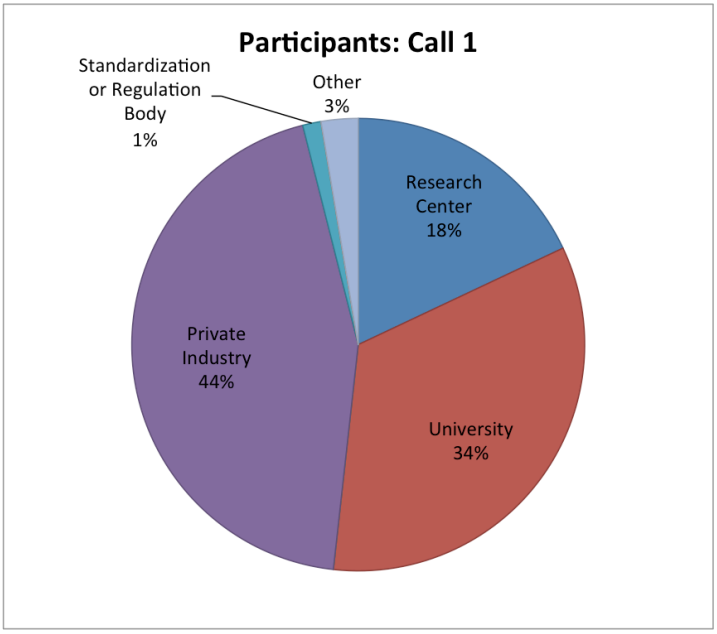

Figure 9. Breakdown of project participants in Call 1

Figure 10 overviews the participants of Call 5 (190 organizations in total). We can remark participation of communes (e.g. the Swedish commune Soderhamn is a participant in the ABC4Trust project of this Call, and the French commune of Nice participates in INSTANT MOBILITY). These actors have appeared due to the projects focused on transport security and projects that run large-scale pilots with end-users.

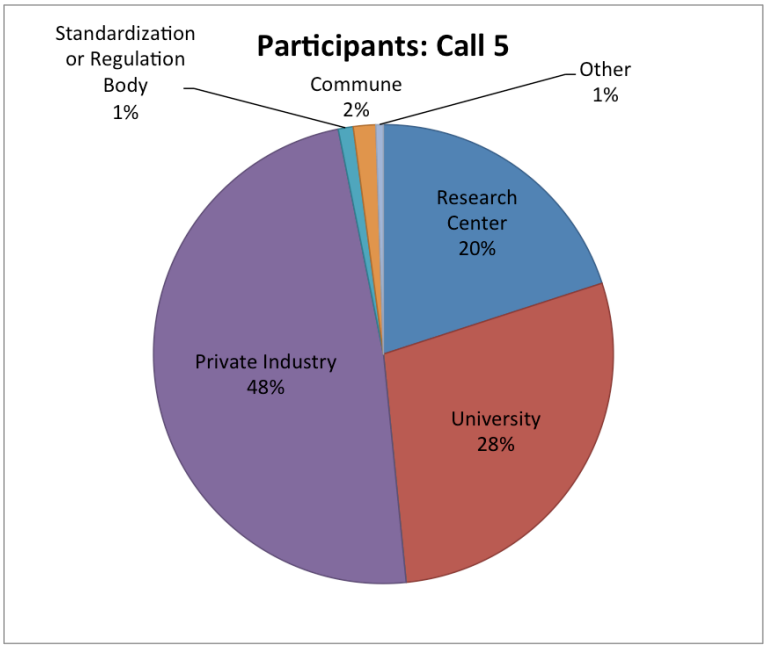

Figure 10. Breakdown of project participants in Call 5

Figure 11 describes the participants landscape in Call 8 that includes 173 organizations. Notice the significant fraction of practitioner alliances that appear in this Call (for example, the UK-based Cloud Security Alliance, Belgian EEMA and LSEC, Spanish AMETIC, etc). We attribute this partially to the share of projects dedicated to pan-European actions (e.g. ACDC, FUTUREID), which require well-managed cross-organizational coordination. Yet this can also be a sign that alliances of security practitioners emerge as a notable actor in the EU R&D projects. They are well-positioned for playing a significant part due to the fact that they already gather experts in the same field but coming from different organizations. Thus a

person or a small company that may not be able to allocate resources for participation in a EU project can become a part of it via an association.

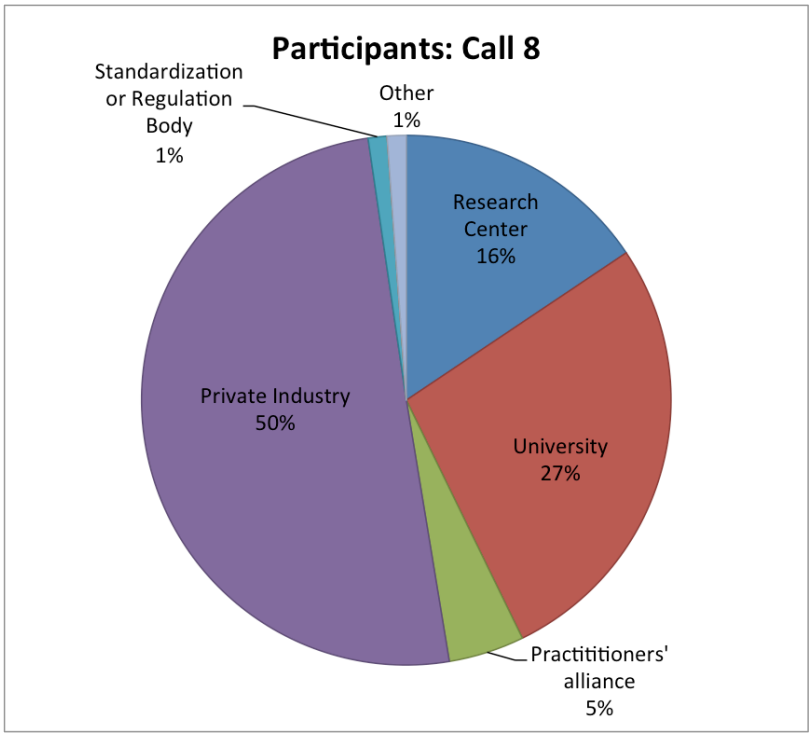

Figure 11. Breakdown of project participants in Call 8

Industries

Figure 12 overviews the domains of private industry organizations participating in the Programme. We classified the companies into ICT integrators (organizations offering a wide range of ICT services tailored to specific business needs of their customers), ICT security companies (organizations with the main focus on security solutions), industry manufacturers (companies that manufacture goods and products), software vendors (companies offering software development services and/or producing generic software), ICT service providers (companies offering web services). Other categories are energy&utility companies; telecom operators and internet service providers; transport and automotive companies; aerospace, defence, military and physical security-oriented companies; organizations offering services such as consulting, insurance and training; companies producing network and telecom equipment (but not manufacturers), and engineering companies. The category “other” in this subsection mainly contains the organizations for which it was not possible to discover their expertise, but also organizations that could not be classified into any other category.

A difficulty with this analysis is potentially incorrect assignment of categories. We have assigned each participating company a single category, while some of them may be attributed to several categories (e.g. the ICT integrators often offer also ICT services and consulting services). Moreover some participating organizations are large, and within this study it was not possible to identity which particular division was taking part in a project: was it a security branch, or a software development unit.

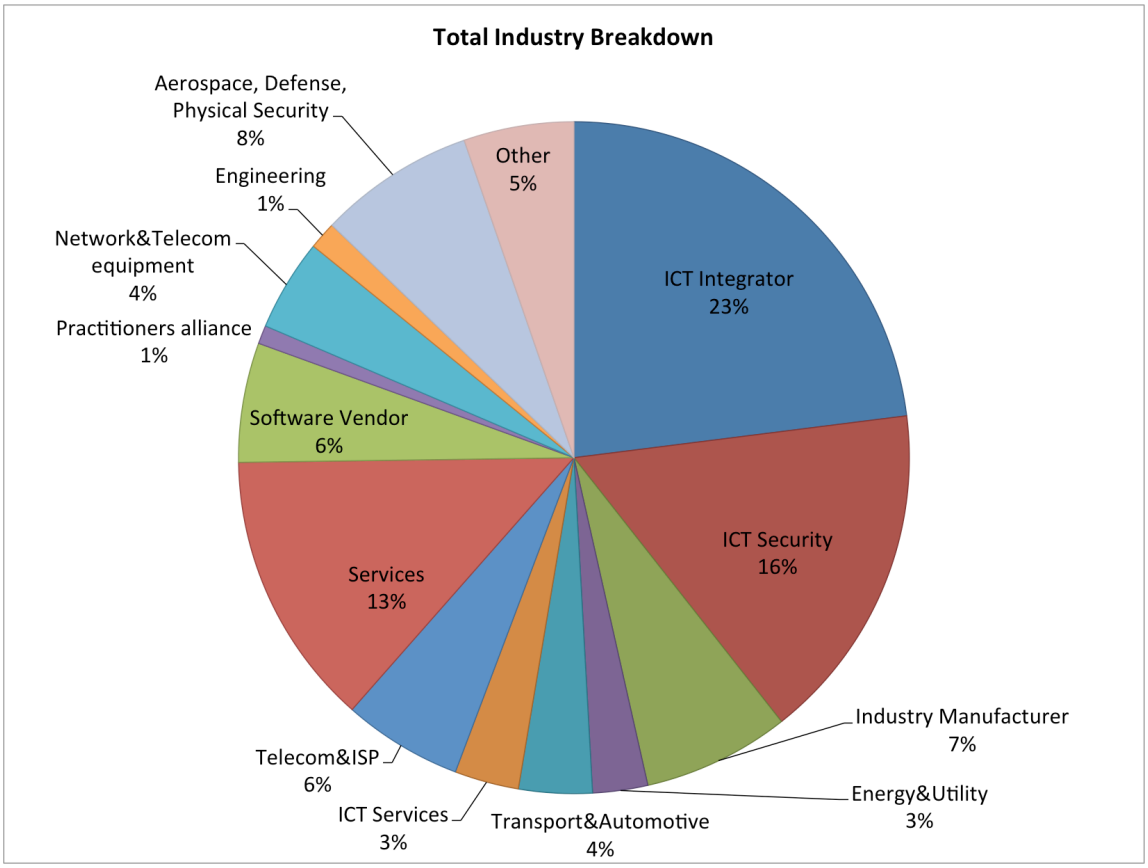

Figure 12. Total breakdown of industry organizations across Calls

Figure 13 breaks down the industry participants of Call 1. We can notice that the participants shares are similar to those of the total breakdown in Figure 12. Call 1 has attracted more utility suppliers than other Calls because it included projects on critical infrastructure protection (e.g. VIKING focused on security of the SCADA systems used in by the electricity suppliers).

Call 5 participants from industry are presented in Figure 14. Note the fraction of transport and automotive companies attributed mostly to the INSTANT MOBILITY project on transport security. Call 5 also attracted more industry manufacturers than any other call due to such projects as SEPIA, TAMPRES and TABULARASA that required competence in manufacturing security products.

Figure 15 presents the industry organizations in Call 8. Energy&utility suppliers do not appear in this Call, but we see the increased shares aerospace&defence companies (impacted by, e.g. the EURO-MILS project that gathers a lot of experts in this domain) and industry manufacturers (due to such projects as EURO-MILS, HINT); and appearance of commercially-oriented practitioners alliances in the picture.

Across the Calls we can see the dominance of ICT integrators, followed by ICT security companies and service providers (mainly consulting companies). Telecom operators and Internet service providers are consistent across the Calls. Industry manufacturers gained bigger shares in Call 5 and Call 8 due to the projects focused on embedded and mobile platforms security.

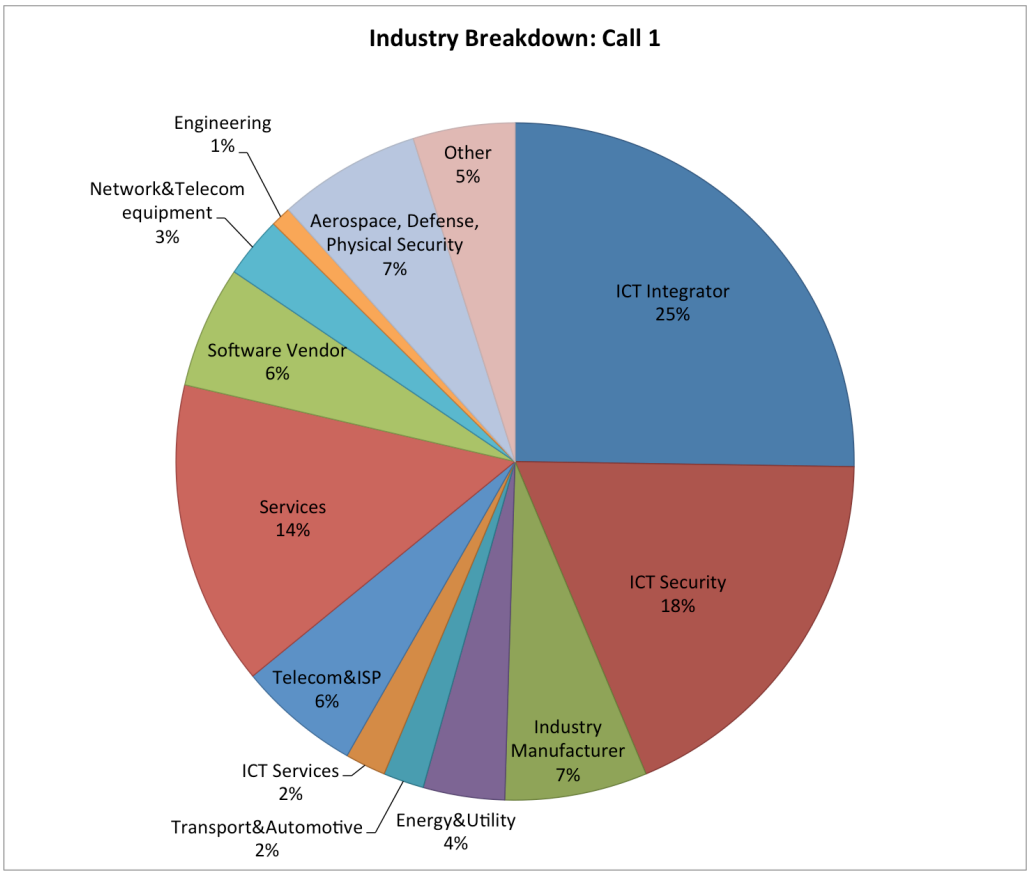

Figure 13. Industry participants in Call 1

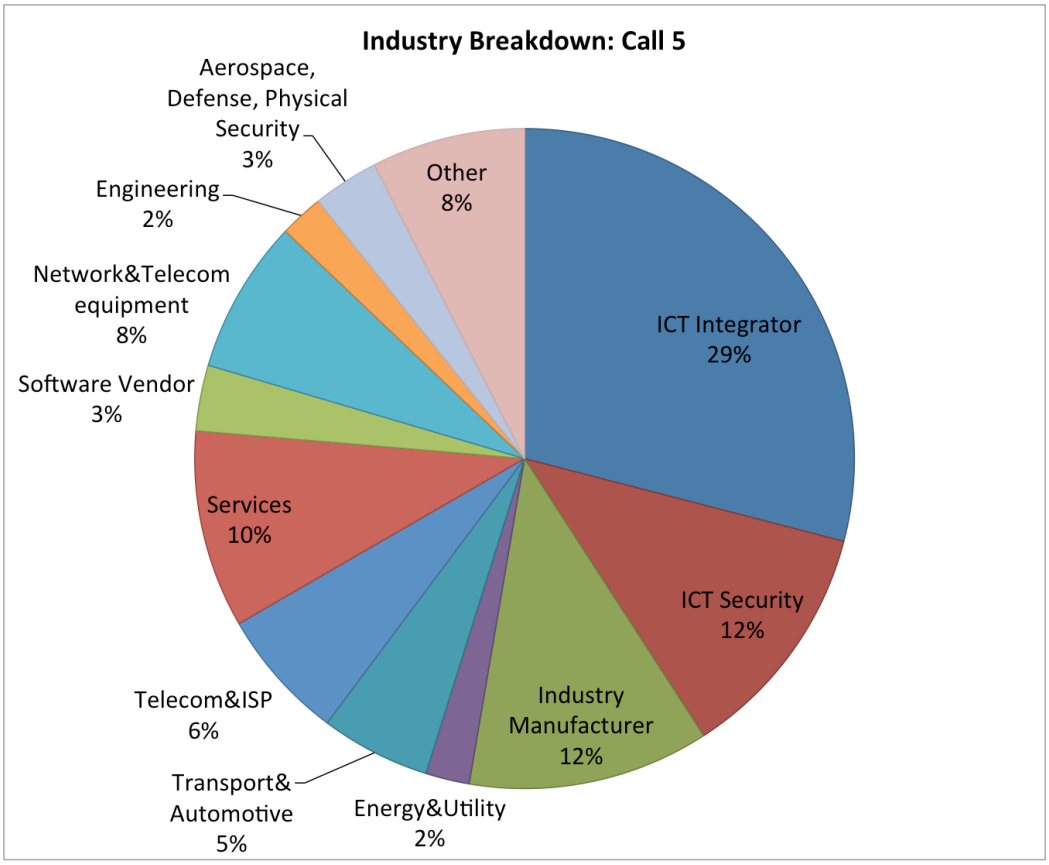

Figure 14. Industry Participants in Call 5

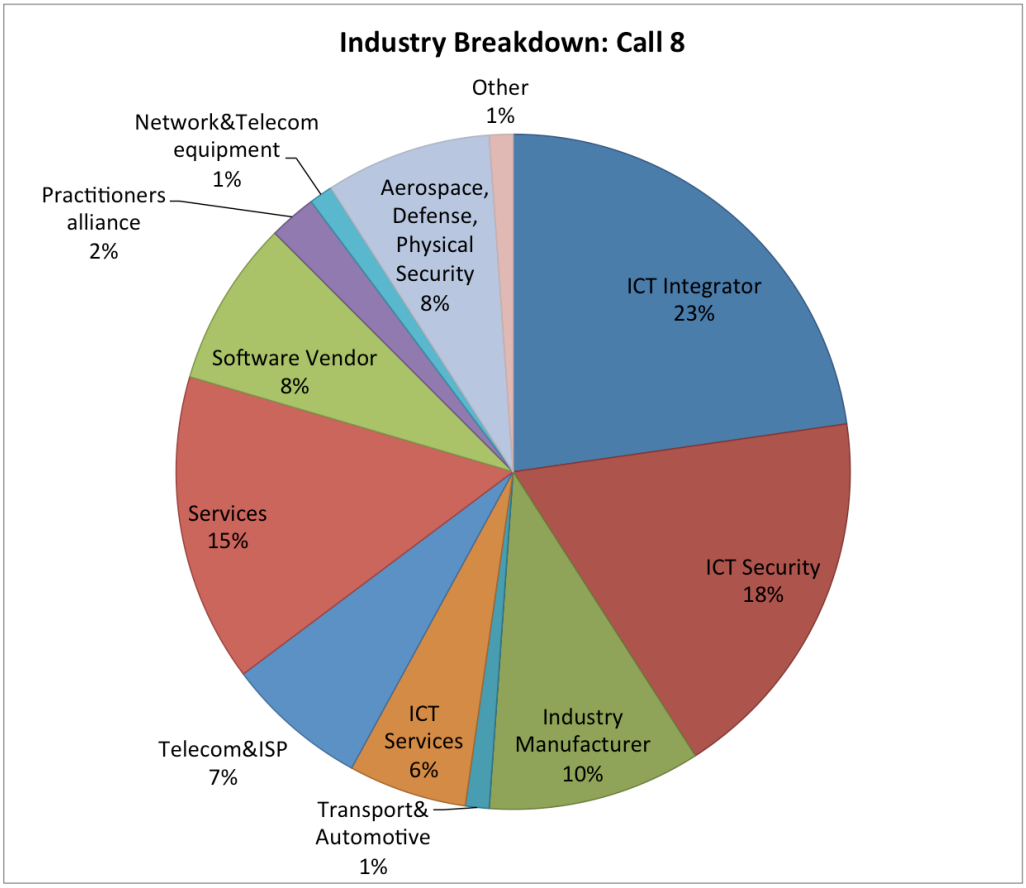

Figure 15. Industry participants in Call 8

Countries

To understand better the European map of projects participants we have executed an analysis of participating countries. Figure 16 plots the participating countries and respective number of project participants coming from these countries for the three Calls. The category "other" includes participants from Israel, Turkey, Russia, US, Australia, Japan and China. The figure demonstrates that Germany brings in the largest share of project participants, followed by France, Italy, UK, Spain and Greece. Notice that this graph is not adjusted neither to the number of participated projects nor to the population.

For all countries participated in a project the median number of organizations is 9; the first quartile is 4 and the 3rd quartile is 19. Table 3 summarizes the countries' contributions. Notice that the number of participants from each country corresponds to the number of different entities participating in the Programme as a whole. Each entity may have contributed to several projects.

To provide a better insight we can notice that for industrial organizations the median number of entities per country across calls is 4, and for research and nonprofit organizations the median per country is 6. Most of the countries fall into the same categories for both types of entities: if the industry participation is high (e.g., in top 25%) than also the research organizations participation is high, and vice-versa.

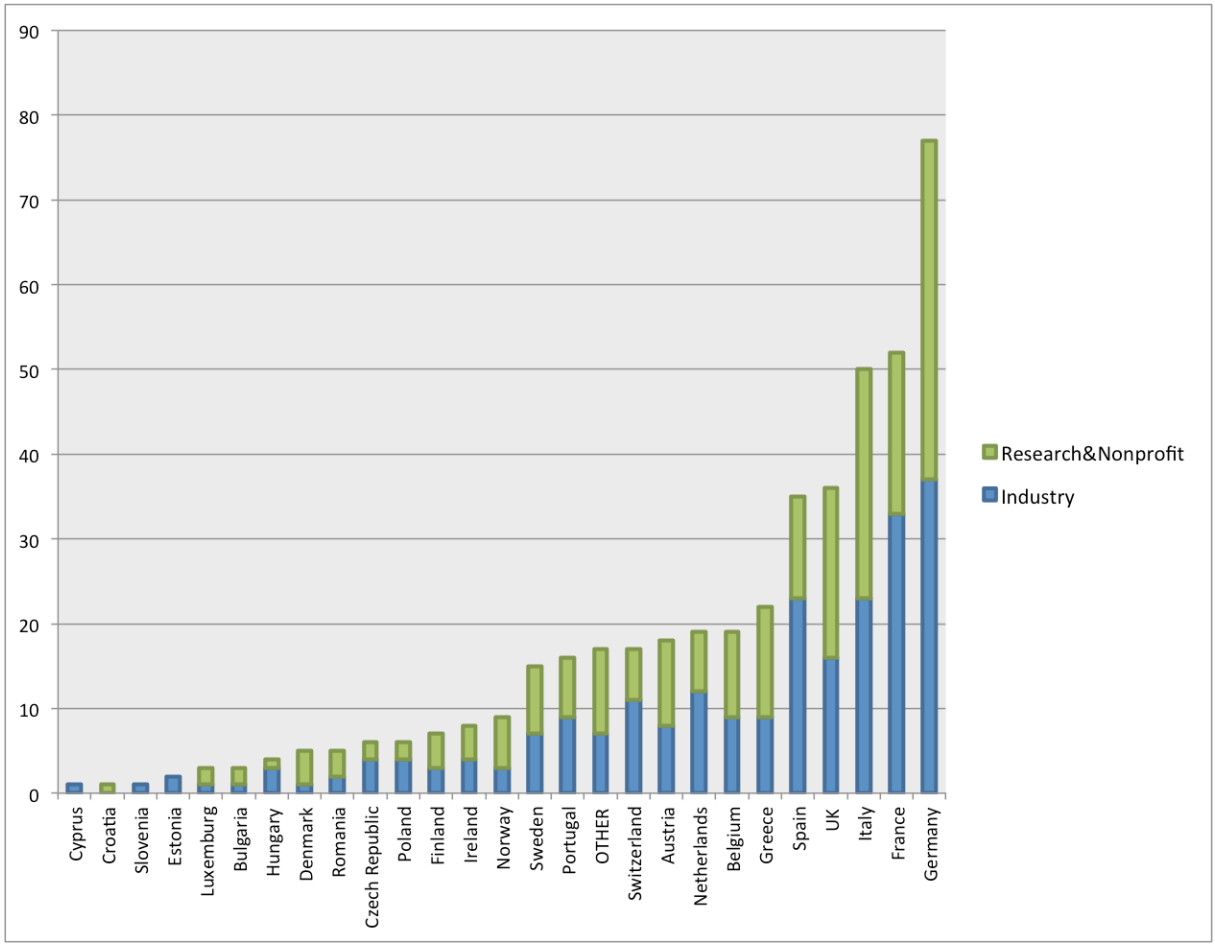

Figure 16. Participation of Countries, across Calls

Table 3. EU countries participation in the Programme

1st quartile countries and respective # of participants		2nd quartile countries and respective # of participants		3rd quartile countries and respective # of participants		4th quartile countries and respective # of participants	
Estonia	2	Ireland	8	Sweden	15	Greece	22
Luxemburg	3	Finland	7	Austria	18	UK	36
Bulgaria	3	Denmark	5	Portugal	16	Spain	35
Cyprus	1	Czech Republic	6	Netherlands	19	Germany	77
Croatia	1	Romania	5	Switzerland	17	France	52
Slovenia	1	Poland	6	Belgium	19	Italy	50
Hungary	4	Norway	9	Other countries	17		

Community Leaders

Across the three Calls the median and the third quartile of participated projects for private industry organizations are equal to 1; thus industry organizations tend to participate in one project (in comparison with research organizations). For research and non-profit

organizations the median for total project participation is 1, but the third quartile is 2; therefore we can say that research organizations tend to participate in more than one project (in comparison with industry). This can be explained by the fact that a single research organization typically hosts a variety of research groups with different interests, which participate in different projects aligned with their profile.

The project participants community includes several outliers (top 5%) with a significant number of projects they have participated in or coordinated. These are the community leaders: some of the most well-connected and well-known organizations in the field of security and trust research in Europe. Notice that top 5%-percentile for project participation across the three Calls consists of organizations that participated in 5 or more projects. For the project coordination, the top 5%-percentile consists of organizations coordinating 2 or more projects. We present the top 5% organizations in the tables Table 4 and

Table 5 below.

Table 4. Top 5% participating organizations across the three Calls

Organization	Number of Participated Projects
ATOS, Spain	18
SAP, Germany	16
Catholic University of Leuven, Belgium	15
Thales, France	12
Waterford Institute of Technology, Ireland	10
IBM Research, Switzerland	9
University of Malaga, Spain	9
SINTEF, Norway	9
Technical University of Darmstadt, Germany	8
ETH, Switzerland	8
EURECOM, France	7
Infineon Technologies, Germany	6
France Telecom, France	6
Telefonica, Spain	6
TECHNIKON, Austria	6
Search-Lab, Hungary	6
Graz University of Technology, Austria	6
ENGINEERING, Italy	5
Selex, Italy	5
Goethe University in Frankfurt, Germany	5
University of Trento, Italy	5
Technical University of Eindhoven, Netherlands	5

Table 5. Organizations - top 5% project coordinators across the three Calls

Organization	Number of Coordinated Projects
Waterford Institute of Technology, Ireland	6
ATOS, Spain	5
TECHNIKON, Austria	5
SAP, Germany	4
Selex Elsag/Elsag Datamat, Italy	2
BICORE, Netherlands	2
University of Verona, Italy	2
SINTEF, Norway	2
Catholic University of Leuven, Belgium	2

Innovation Projects Highlights

The project highlights presented in this section are a result of a study conducted by UNITN. For each Call we have investigated different aspects of the participating projects. We have conducted interviews with coordinators of projects in Call 5 and Call 8 (when they agreed to this) to find more information regarding the key innovative results expected and technology acceptance gaps envisioned.

For the study only the projects that aimed to produce scientific results were selected, thus the projects from the Networking, Coordination and Support category (excluding the Networks of Excellence) from Call 5 and Call 1 were not contacted (such as INCO-TRUST, BIC, THINKTRUST, etc). Also some of the projects from Call 1 with not working websites were not contacted due to their obvious lack of interest to promote the project results (if they did not reply even in the EFFECTS+' study); and the projects from the ICT-FI Call were not contacted because they have somewhat different goals.

However, the projects in Call 8 from the Networking, Coordination and Support category were contacted to identify their goals; only SECCORD was excluded due to the possibility of bias; and the ACDC project was not contacted because it was not possible to find its contact details at the time of the study (it does not have a dedicated page in the CORDIS system, and the search engines have identified its webpage only very recently).

For Call 1 it was difficult to organize the study due to the fact that the projects have finished several years ago. Some projects' websites are already not maintained; the former project coordinators often have changed affiliations and are not willing to disseminate the projects' technologies anymore. Therefore the presented information for projects of Call 1 is shorter.

The presented project contact details (the tables) were taken from projects' websites, where it was possible, and may differ from the CORDIS information.

Call 1 and Joint ICT-SEC Call

Project Presentation Outline

For the projects of Call1 and ICT-SEC information for each project includes a short summary from CORDIS, followed by presentation of the project's objectives and main innovation achievements, as well as discussion of possible concrete impacts from the project grounded on the validation activities executed in the project, pointers to interesting publications and follow-up projects (if any). Notice that the innovation targets and impacts for projects in Call 1 were elicited by UNITN.

Projects reported in this section:

- AVANTSSAR
- CONSEQUENCE
- MASTER
- MICIE
- PICOS
- UAN
- VIKING

Projects that are not reported in this section:

- ACTIBIO
- AMBER
- AWISSENET
- CACE
- COMIFIN
- ECRYPT II
- FORWARD
- GEMOM
- INCO-TRUST
- INSPIRE
- INTERSECTION
- MOBIO
- PARSIFAL
- PEACE
- PRIMELIFE
- PRISM
- SECURESCM
- SERSCIS
- SHIELDS
- SWIFT
- TAS3
- TECOM
- THINKTRUST
- TURBINE
- WOMBAT
- WSAN4CHIP

Information regarding the projects above can be found in the CORDIS system [1].

AVANTSSAR

Acronym	AVANTSSAR
Project	Automated VAlidatioN of Trust and Security of Service-oriented ARchitectures
Dates	2008-01-01 to 2010-12-31
Participants Number	10
Coordinator	University of Verona, Italy
Other participants	ETH Switzerland, INRIA Nancy France, IRI Toulouse France, University of Genoa Italy, IBM Research Lab Switzerland, OPENTRUST France, Institute e-Austria Timisoara Romania, SAP Germany, Siemens Germany
Website	http://www.avantssar.eu
Classification in CORDIS	Trustworthy Service Infrastructures

Objectives

Driven by rapidly changing requirements and business needs, IT systems and applications are undergoing a paradigm shift: components are replaced by services, distributed over the network, and composed and reconfigured dynamically in a demand-driven way into service-oriented architectures. Exposing services in future network infrastructures entails a wide range of trust and security issues. Therefore there is a need for validation of both the service components and their composition into secure service architectures.

AVANTSSAR has proposed a rigorous technology for the formal specification and automated validation of trust and security of service-oriented architectures. This technology was automated into an integrated toolset, the AVANTSSAR validation platform, tuned on relevant industrial case studies.

Innovation targets

The project has developed:

- 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 dynamic composite services, and their associated security policies.
- 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 our technology scales to envisaged applications.

Impact

Migrating project results to industrial development environments and standardization organizations may 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. The project has included the WP6 Industry Migration to facilitate exploitation of the AVANTSSAR results; experiences and lessons learned during the AVANTSSAR technology migration are presented in the deliverables of this work package.

Have a look at

The AVANTSSAR platform is accessible at the project website, including a comprehensive user manual. A report on the platform was presented in the paper “The AVANTSSAR Platform for the Automated Validation of Trust and Security of Service-Oriented Architectures” by A. Armando et al. presented at the 18th International Conference on Tools and Algorithms for the Construction and Analysis of Systems (TACAS’2012)

Next steps

The SPaCIoS project (Call 5) is a follow-up project of AVANTSSAR.

CONSEQUENCE

Acronym	CONSEQUENCE
Project	Context-aware data-centric information sharing
Dates	2008-01-01 to 2010-12-31
Participants Number	7
Coordinator	Microsoft Innovation Center Europe, Germany
Other participants	BAE Systems UK, HP Italy, Imperial College London, The Science and Technology Facilities Council UK, CNR Italy, Create-Net Italy
Website	http://www.consequence-project.eu
Classification in CORDIS	Trustworthy Service Infrastructures, Technology&Tools

Objectives

The CONSEQUENCE project has worked on a data-centric information protection framework based on data-sharing agreements. While data exchange is vital for the society today it is often hindered by privacy and confidentiality threats associated with unauthorized data sharing. The CONSEQUENCE project devised its framework for data sharing taking into account not only technological, but also economical and social aspects of data exchange.

Innovation targets:

CONSEQUENCE has achieved:

- A scalable, secure, context-aware and resilient architecture for data sharing that enables dynamic policy management and enforcement, and end-do-end data protection across multiple organizations.
- A technique for organization-neutral data sharing agreements (including models, algorithms and tools).
- A proof-of-concept implementation of the CONSEQUENCE data-sharing framework.

Impact

The project has especially focused on data sharing in emergency situations. One of the test cases used in the project for validation was a critical management testbed provided by BAE systems. Evaluation of the CONSEQUENCE system on this testbed is reported in D5.4 of the project. The project's results may prove useful in the emergency situations context, as well as in the context of sensitive data sharing across multiple companies.

Have a look at

Demonstration videos of the CONSEQUENCE technology are available at the project website http://www.consequence-project.eu/press_center.html

Find out more details about the CONSEQUENCE technology in crisis management scenarios in the paper "An Opportunistic Authority Evaluation Scheme for Data Security in Crisis Management Scenarios", by E. Scalavino, G. Russello, R. Ball, V. Gowadia, E. Lupu in Proceedings of the 5th ACM Symposium on Information, Computer and Communication Security (ASIACCS'2010).

MASTER

Acronym	MASTER
Project	Managing assurance, security and trust for services
Dates	2008-02-01 to 2011-01-31
Participants Number	14
Coordinator	ATOS Spain
Other participants	SINTEF Norway, IBM Research Lab Switzerland, University of Stuttgart Germany, ETH Switzerland, University of Trento Italy, Dublin City University Ireland, British Telecom UK, ANECT Czech Republic, ENGINEERING Italy, San Rafaele Foundation Italy, Deloitte France, CESCE Spain
Website	Website is not maintained http://www.master-fp7.eu
Classification in CORDIS	Trustworthy Service Infrastructures

Objectives

The MASTER project aimed at developing a system for ensuring compliance with regulations, internal policies and contractual obligations by an organization. Today organizations may have quite complex and unpredictable business processes, while accountability and regulatory compliance have widely become mandatory. Therefore a structured and possibly automated approach to governance, risk and compliance (GRC) is a goal for many companies. MASTER has fulfilled this demand by delivering a system that assists compliance management in many aspects: by monitoring organizational performance, enforcing policies and assessing the compliance level.

Innovation targets

MASTER has delivered the following key results:

- The MASTER methodology that describes how an organization can derive specific activities to be done and control objectives from high level regulations and policies (delivered in work package 8.2)
- The MASTER design workbench – a tool to translate high-level regulations and policies into low-level policies that control management process in an organization. The tool was delivered in work package 8.3

Impact

The MASTER approach can increase security in organizations and ensure compliance with the EU regulations and industry standards. Some parts of the MASTER methodology can be used as an input to a compliance assessment process standard. The project has validated its results on two case studies – in an insurance company and in a hospital.

Have a look

The MASTER methodology for implementing controls at the business process level by the GRC triad was published in the ISACA Journal, one of the most recognized magazines for the GRC practitioners. Read the article “Realizing Trustworthy Business Services Through a New GRC Approach” by Y. Asnar et al. in the ISACA Journal Vol. 2 (2010)

MICIE

Acronym	MICIE
Project	Tool for systemic risk analysis and secure mediation of data exchanged across linked CI information infrastructures
Dates	2008-09-01 to 2011-02-28
Participants Number	11
Coordinator	Selex Italy
Other participants	University of Coimbra Portuagal, University of Bradford UK, Henri Tudor Research Center Luxemburg, CRAT University of Rome Italy, University of Rome Tre Italy, ENEA Italy, PIAP Poland, Israel Electric Corp, itrust consulting Luxemburg, Multitel ASBL Belgium
Website	http://www.micie.eu
Classification in CORDIS	Critical Information Infrastructure Protection

Objectives

The MICIE consortium was contributing to the Critical Infrastructure (CI) protection. Critical Infrastructures can be damaged by malicious activities or natural disasters. Disruptions in the CI facilities can be a serious threat to the society. It is therefore crucial to ensure security and reliability of CIs as well as to be able to have disaster notification and recovery services in place. The MICIE project has developed an alerting system to identify in real time the level of possible threats induced on a particular CI or on other interdepended critical facilities, and notify the authorities providing them a real risk level.

Innovation targets

MICIE has produced the alerting system including the following innovative components:

- The off-line design of critical infrastructure models that are able to detect dominant dynamics from a series of occurring undesired events.
- The MICIE secure mediation gateways responsible for collection of undesired events, translation of these events into a common meta-data model and exchange of the meta-data.
- The MICIE on-line risk prediction tool that is able to predict the risk levels in real time from the CI models and the meta-data received.

Impact

The MICIE project results are directly in line with the EU initiative to establish a Critical Infrastructure Warning Information Network (CIWIN), contributing to safety of the EU society.
The energy distribution domain was chosen as an application for validation of the project results. The project has evaluated whether the MICIE tool could increase the quality of service in this domain. After analyzing the communication fault events and their influence on the quality of service of the electric energy supply in presence of the MICIE tool and without it, the consortium has concluded that the MICIE technology can increase the quality of service by assisting the operator in identifying faults and countermeasures.

Have a look

The article “Agent Based Input-Output Interdependency Model” by G. Oliva, S. Panzieri and R. Setola was published in the International Journal on Critical Infrastructure Protection (Elsevier) Vol.3(2), 2010.
The paper “A SVM-Based Behavior Monitoring Algorithm towards Detection of Un-desired Events in Critical Infrastructures” by J. Jiang, P. Capodieci, J. Yang, has been published in the book *Advances in Intelligent and Soft Computing* (ISSN: 1867-5662) Editor Springer Berlin

PICOS

Acronym	PICOS
Project	Privacy and identity management for community services
Dates	2008-02-01 to 2011-01-31
Participants Number	11
Coordinator	Goethe University in Frankfurt, Germany
Other participants	HP France, Deutsche Telecom Germany, ATOS Spain, University of Malaga Spain, CURE Austria, Catholic University of Leuven Belgium, IT-Objects Germany, Leibniz Institute of Marine Sciences Germany, Masaryk University in Brno Czech Republic
Website	http://www.picos-project.eu
Classification in CORDIS	Privacy Management

Objectives

The main goal of the PICOS project was to advance the state-of-the-art in technologies providing privacy-enhanced identity and trust management features within complex services such as online communities managed by mobile communication service providers. PICOS aimed at building and trying out with real users of a privacy-respecting identity management platform that supports provision of online community services and a client application for this platform.

Innovation targets

PICOS has delivered the following innovative technologies:

- The Partial Identity concept that allows users to reveal only selected personal information as their identity (e.g. a position at a company or a social role).
- The Privacy Advisor tool to guide the users in aspects of their privacy and identity management, for example to raise early warnings before the user discloses personal information in an unsecure context.
- A privacy-friendly targeted advertising technology.
- The PICOS platform that combines the aforementioned technologies and an accompanying mobile phone client to serve as a user interface.

Impact

The PICOS results can support developments in the EU policy and regulations for privacy protection and protection of minors on the Internet. The project has run pilots with real end-users from an online gaming community and an angler community and has gained a lot of insights of the society requirements on privacy.

Have a look at

Watch the demonstration videos of some of the project's results at the website http://www.picos-project.eu/Concepts-Features.204.0.html

UAN

Acronym	UAN
Project	Underwater acoustic network
Dates	2008-10-01 to 2011-09-30
Participants Number	6
Coordinator	CINTAL Portugal
Other participants	SELEX Italy, SINTEF Norway, FOI Swedish Defense Research Agency Sweden, ISME at University of Genova Italy, KongsBerg Maritime Norway
Website	http://www.ua-net.eu
Classification in CORDIS	Critical Information Infrastructure Protection

Objectives

UAN was developing a wireless sensor network for protection of off-shore and coastline critical infrastructures (CI). The acoustic network developed by UAN includes underwater, land and air-based sensors in order to gather environmental information for surveillance, monitoring and deterrence.

Innovation targets

UAN has produced the next key innovative results:

- The UAN acoustic modems, gateway access point, a ground station and accompanying software.
- The full UAN network demonstrator.

Impact

The UAN acoustic framework was the first one of its kind with fixed and mobile nodes that was seamlessly integrated in a land communication network. The project has demonstrated with two real seal experiments that the UAN network is fully operational. Potential beneficiaries of the UAN network deployments are search and rescue operation bodies, port authorities, oil and gas exploration entities, marine scientists and military units.

Have a look at

Find out more details about one of the UAN sea deployment trials in the article “Mobile Underwater Sensor Networks for Protection and Security: Field Experience at the UAN11 Experiment”, by A. Caiti et al. published in Journal of Field Robotics, 30(2), 2013.

VIKING

Acronym	VIKING
Project	Vital infrastructure, networks, information and control systems management
Dates	2008-11-01 to 2011-11-30
Participants Number	7
Coordinator	ABB Germany
Other participants	E.ON Germany, ETH Switzerland, MML Analysis and Strategy Sweden, The University System of Maryland Foundation US, KTH Sweden, Astron Informatikai Hungary
Website	http://www.vikingproject.eu
Classification in CORDIS	Critical Information Infrastructure Protection

Objectives

The VIKING project investigated cyberthreats on SCADA systems that control electricity supply and proposed mitigation against exploits of these threats. Society is highly dependent on electricity grids, which are large-scale and complex systems that need to be always reliable, available and cost-effective. VIKING worked towards a holistic framework for identification and assessment of vulnerabilities in SCADA systems and for estimation of societal consequences from power breakdowns.

Innovation targets

VIKING has developed the next key innovations:

- A system to run model-based risk assessment for SCADA systems.
- A set of quantitative metrics for cybersecurity for different control system solutions.
- Estimation of vulnerabilities in higher order applications like State Estimators and Automatic Generation Control and suggestions for mitigations to these threats
- Secure communication solutions
- The ViCiSi simulator of a virtual society used for calculation of economical and non-economical consequences from electrical blackouts
- A testbed that can be used to simulate and demonstrate cyberattacks on SCADA systems.

Impact

The results of the VIKING project are of high importance for the EU society and governments. The experiments with the VIKING simulator can be used to estimate the impact of potential attacks on national welfare. The industrial partners plan to use parts of the findings in their commercial offerings and in the operation of their power networks.

Have a look at

The VIKING project produced more than 40 scientific papers and articles describing different aspects of the VIKING research that have been presented in international magazines and at conferences.

The results of the project are summarized in the VIKING final report available on the VIKING web page. Furthermore, the project has made a movie illustrating one of the VIKING Story Boards: http://www.youtube.com/watch?v=Y_ifu65FdXo (also available at the project website).

Call 5 and ICT-FI Call

Project Presentation Outline

For the projects of Call 5 the presentation follows the following structure. For each project we present a short summary details from CORDIS, a summary of project objectives in comparison with the state of the art and the key innovative contributions achieved. We also discuss possible market acceptance gaps, as envisaged or experienced by the project itself, followed by the mitigation strategies executed by the consortium. We then overview potential impacts from the project on technology, standards, policies and society in general, and provide some more details about the validation and dissemination activities run by the projects, and some interesting highlights the project wished to share. The presented information is based on personal interviews with project leaders.

In this section the following projects are described:

- ABC4TRUST
- ANIKETOS
- ASSERT4SOA
- MASSIF
- POSECCO
- SYSSEC
- TAMPRES
- UTRUSTIT

The following projects are not reported in this section:

- ACTOR
- BIC
- DEMONS
- EFFECTS+
- ENDORSE
- ENVIROFI
- GINI-SA
- INSTANT MOBILITY
- NESSOS
- PASSIVE
- PINCETTE
- SAFE CITY
- SECFUTUR
- SEPIA
- SPACIOUS
- TABULA RASA
- TCLOUDS
- TWISNET
- VIS-SENSE
- WEBSAND

Information regarding the projects listed above can be found in the CORDIS system [1].

ABC4TRUST

Acronym	ABC4TRUST or ABC4Trust
Project	Attribute-based Credentials for Trust
Dates	2010-11-01 to 2014-10-31
Participants Number	12
Coordinator	Goethe University in Frankfurt, Germany
Other participants	CryptoExperts France, Technical University of Darmstadt Germany, Alexandra Institute Denmark, ULD Germany, CTI Greece, Eurodocs Sweden, IBM Research Switzerland, Miracle Denmark, Soderhamn Commune Sweden, Nokia Siemens Networks Germany, Microsoft Belgium
Website	https://abc4trust.eu
Classification in CORDIS	Trustworthy Service Infrastructures, Privacy Management

Objectives

The ABC4Trust project enhances privacy in the Internet by developing attribute-based credentials.

Currently credentials used to authenticate or identify a user were often not designed to respect her privacy. They usually reveal the full identity of the credential holder even if an application that demands credentials often needs much less information. For example, vending machines often require only the confirmation that the holder is older than 18. The situation of fully revealing the identity when it is not necessary is not compliant with the privacy standards of minimal disclosure. Attribute-based credentials developed by ABC4Trust allow users to reveal just the minimal information required by the application, without giving away full identity information.

Innovation Achievements

The project works on delivering the key artefacts specified below:

- The ABC4Trust reference architecture for attribute-based credentials, which is a new privacy-enhancing authentication technology.
- Prototype implementations of attribute-based credentials schemes, which are validated by large-scale pilots with end-users.
- Smart card-based operations with attribute-based credentials and prototype systems of an Issuer and a Verifier.

Market acceptance gaps

The ABC4Trust technology can be unfamiliar to end-users, and they may have reservations against using it. These reservations were captured in the beginning of both pilots.

Mitigation strategies

The project has conducted dedicated seminars with pilot participants to explain the idea and the technology behind the new credential schemes. After the seminars users have shown more trust in the deployed system. From this experience and from market studies conducted ABC4Trust considers the attribute-bases credentials technology can be easily adopted by the EU citizens after they are introduced to it.

Impact

The project results are expected to impact existing standards in the electronic identity management schemes as well as existing security laws. For instance, the project actively participates in the debates on the new EU Electronic Identification and Trust Services Regulation.

Adoption of the attribute-based credentials will allow end-users to protect their privacy and reveal only the minimal information required, therefore leading to more privacy-protecting yet trustworthy identification systems in digital society. The users will become empowered with reassurance that their identity is at their hands.

Zoom in

The industrial players in the consortium (Nokia Siemens Network, IBM and Microsoft) already consider adoption of the attribute-based credentials technology in their products, being inspired by very positive feedback from the EU leading experts in security as well as pilot end-users.

The pilot studies executed by the project are quite diverse. The first pilot is run at a Greek university with around 60 students. The attribute-based credentials framework deployed by the project allows the students to participate anonymously in an online course evaluation system. The second pilot is run with pupils of a Sweden school who can access community services (focused on online communications between community members) while their privacy is protected by enabling pseudonymous and anonymous access.

Have a look at

The ABC4Trust is promoting privacy-protecting identity systems to be explicitly introduced in the new Regulation on Electronic Identification and Trust Services. Read the project position paper at https://abc4trust.eu/index.php/news/archived-news/159-eidas

ANIKETOS

Acronym	ANIKETOS
Project	Secure and Trustworthy Composite Services
Dates	2010-08-01 to 2014-01-31
Participants Number	17
Coordinator	SINTEF Norway
Other participants	ATOS Spain, Athens Technology Center (ATC) Greece, DAEM Greece, DeepBlue Italy, SELEX Italy, CNR Italy, Italtel Italy, Liverpool John Moores University UK, SAP Germany, SEARCH-LAB Hungary, Tecnalia Spain, Thales France, Waterford Institute of Technology Ireland, University of Trento Italy, WIND Italy, ICT&S Center at University of Salzburg Austria
Website	http://www.aniketos.eu
Classification in CORDIS	Trustworthy Service Infrastructures

Objectives

Users of service mashups typically have low assurance of what service they are actually using and whether it is secure and reliable. Future Internet will likely worsen this situation, with more services offered for dynamic consumption and composition based on service availability, quality, price and security attributes. Applications will be composed of multiple services from many different providers, and the end user may have little guarantee that a particular service will actually deliver the security claimed (if any). The ANIKETOS project aims to establish and maintain trustworthiness and secure behaviour of services in a constantly changing environment.

Innovation Achievements

ANIKETOS works on the following innovative artefacts:

- A language to express security and trustworthiness requirements on socio-technical systems: the Socio-Technical Security Modelling Language (STS-ml) and the accompanying tool (STS-tool).
- The security-by-contract paradigm for services that enables services to express their security and trust requirements in their machine-readable contracts.
- The ANIKETOS platform and accompanying tools to support service designers in building composite services that meet security requirements, and system administrators to monitor execution of composite services and react in case of violations.

Market acceptance gaps

Acceptance of the ANIKETOS technology in the security practitioners' community may be hindered by lack of awareness of the technology benefits. Another aspect acknowledged by the project that might hinder adoption is the intellectual property rights of individual project partners that might not want to fully disclose the developed technology and software.

Mitigation strategies

ANIKETOS actively disseminates its results to potential stakeholders. The project comprises a specific work package WP11 that deals with exploitation strategies for each individual partner.

To increase the ANIKETOS technology viability the project considers further enhancements to the platform – a service marketplace and a threats repository, and investigates suitable business models to attract service providers and designers.

Impact

Adoption of the ANIKETOS framework will bring assurance of trustworthiness to service consumers, which are not only individual end-users, but also composite service designers and providers. The ANIKETOS approach adoption will facilitate the European service marketplace.

Zoom in

ANIKETOS runs three case studies: air-traffic management, e-government and telecom services selected to demonstrate value of the project's contributions in a variety of domains.

The project comprises several work packages completely dedicated to dissemination and promotion of project results. These are Training (WP8), Demonstration (WP9), Community (WP10) and Dissemination/Exploitation (WP11).

Have a look at

ANIKETOS has demonstrated some of its key artefacts on the IEEE stand at the International CES Show 2013 with more than 150,000 of attendants.

Find out more details at http://www.aniketos.eu/content/aniketos-demonstrations-ces-and-ccnc

Discover more details of STS-ml and the STS-tool at http://www.sts-tool.eu

ASSERT4SOA

Acronym	ASSERT4SOA
Project	Advanced Security Service cERTificate for SOA
Dates	2010-10-01 to 2013-09-30
Participants Number	7
Coordinator	SAP Germany
Other participants	University of Milan Italy, The City University UK, ENGINEERING Italy, University of Malaga Spain, Ugo Bordoni Foundation Italy, SIT at Fraunhofer Germany
Website	http://www.assert4soa.eu
Classification in CORDIS	Trustworthy Service Infrastructures

Objectives

ASSERT4SOA focuses on security certification for service-based applications. Today the Service-Oriented Architecture (SOA) paradigm has become a de-facto architectural standard for deployment of dynamic large-scale infrastructures and applications consisting of independent modules – services. The benefits of this paradigm include flexibility, cost-effectiveness and ease of modules replacement. Yet deployment of SOA-based solutions in the domain of sensitive and critical applications is limited due to absence of guarantees that composite third-party services are secure. In the conventional software domain security certification is used for guaranteeing security and trustworthiness of a software component. ASSERT4SOA aims to produce security certification standards for services, taking into account the dynamic nature of services and tackling assurance for service compositions.

Innovation achievements

Certification for services is a very new topic with few existing proposals. The project has delivered the following key artifacts:

- The machine-readable description language called ASSERT for service security certificates.
- The ASSERT architecture that enables an ontology-based format for certificates and supports linking of security properties to evidence supporting them. The architecture allows run-time certificate-aware service selection based on a target assurance level for composite applications.
- The ASSERT4SOA integrated prototype that implements an ASSERT-enabled service marketplace.

Market acceptance gaps

Security certification is currently considered to be an expensive process only suitable for highly critical applications. The customers may not want to invest into certification for less critical applications, or are even unaware that certification for services exists.

The existing service standards do not define a way to express service certificates, therefore the ASSERT language may not be recognized by existing service platforms. Acceptance of service certification can be only enabled through a dedicated ecosystem.

Mitigation strategies

The project enables lightweight and cost-effective certification for services. The business community and customers are outreached through dedicated workshops, targeted demonstrations and presentations at developer conferences. The ASSERT4SOA results will be also taken over by another EU R&D project.

To standardize the ASSERT language the project interacts with the ETSI group.

Impact

Certification for SOA enables more trustworthy services and composite service-based applications. The ASSERT framework also aligns well with the upcoming EU Data Protection Regulation where certification is mentioned explicitly.

Zoom in

ASSERT4SOA performs validation of its results with three dedicated focus groups. The first focus group consists of software developers that work with composite service applications. Developers will evaluate how well the ASSERT platform suits their needs for providing assurance about services they include into their business processes. Second focus group consists of people involved in procurement, which are interested in buying solutions with certain assurance levels. The third group is composed of certification bodies employees that assess the ASSERT certification process.

Have a look at

Discover the ASSERT language for service certificates at the project website http://www.assert4soa.eu/public-deliverables/102-languagev21

MASSIF

Acronym	MASSIF
Project	MAnagement of Security information and events in Service InFrastructures
Dates	2010-10-01 to 2013-09-30
Participants Number	12
Coordinator	ATOS Spain
Other participants	SPIIRAS Russia, T-Systems South Africa, SIT at Fraunhofer Germany, Polytechnic University of Madrid Spain, CINI Italy, AlienVault Spain, FFC at University of Lisbon Portugal, Orange Labs - France Telecom, 6CURE France, Epsilon Italy, Telecom SudParis France
Website	http://www.massif-project.eu
Classification in CORDIS	Trustworthy Service Infrastructures

Objectives

MASSIF works on advancements in security information and event management systems (SIEM) that deal with real-time analysis of events and security alerts. Standard SIEM systems typically are deployed at a platform layer and they do not take into account data from higher layers, such as the business process view. Being usually deployed on a single node responsible for processing all event correlation rules, they are not scalable. Moreover, existing systems are not able to react to detected attacks.

Innovation achievements

The MASSIF SIEM framework supports scalable multi-level event processing and predictive security monitoring. The key innovative artefacts are:

- Advanced attack detection methods.
- Cross-layer security event correlation and decision support for analysis of possible impacts an attack may have on the system.
- Predictive security monitoring that detects potential future critical states in the monitored process.
- Attack response mechanisms that propose countermeasures based on security ontologies.
- The MASSIF SIEM architecture that integrates the components above in a secure and reliable way.

Market acceptance gaps

The MASSIF consortium has faced the following gaps:

- Deployment of a SIEM solution to a new system can be hindered by differences in existing IT systems and their event collection mechanisms, since adapting to a new platform can take significant time.
- Consumers are unaware of the potential of SIEM systems and are reluctant to deploy them.

Mitigation strategies

The modularity of the MASSIF platform where each component is independent from others allows to easily reconfigure MASSIF for each new platform.

The MASSIF team overcomes consumer unawareness by demonstrating the solutions and their potential to customers, including potential customers from the project Advisory Board.

Impact

MASSIF provides two open source implementations of SIEM solutions called OSSIM and Prelude, which can be further used by the community. The MASSIF approach can make total cost of ownership of a SIEM system affordable for SMEs due to the open specifications and open source components available.

The project contributes to the ETSI Information Security Indicators group that aims at measuring security levels of organizations with deployed SIEM systems.

Deployment of SIEM systems in critical infrastructures has a huge potential, especially in the light of the Directive on Critical Infrastructures Protection.

Zoom in

Four industrial scenarios are used in MASSIF:

- Olympic Games IT infrastructure deployed and managed by ATOS that demands high scalability.
- France Telecom provides a scenario on mobile phone-based money transfer service facing security events, especially for the "non-IT" and "service" events.
- T-Systems South Africa provides managed IT outsource services with a high degree of complexity in setting up SIEM systems for large distributed enterprises.
- Epsilon demonstrates the use of the advanced concepts of SIEM in an IT system supporting a critical infrastructure (dam). This is one of the first deployments of a SIEM system on critical infrastructures.

Have a look at

MASSIF shares the design guidelines on its website http://www.massif-project.eu. Contact the project for the open source implementation of innovative SIEM components.

POSECCO

Acronym	PoSecCo
Project	Policy and Security Configuration Management
Dates	2010-10-01 to 2013-09-30
Participants Number	11
Coordinator	SAP Germany
Other participants	University of Bergamo Italy, CrossGate Germany, University of Innsbruck Austria, IBM Research Switzerland, ATOS Spain, Technical University of Eindhoven Netherlands, Deloitte France, Polytechnic University of Turin Italy, Bern University of Applied Sciences Switzerland, Thales Services France
Website	http://www.posecco.eu
Classification in CORDIS	Technology&Tools

Objectives

Today, Internet service providers have to manually resolve inter-dependencies between high-level security requirements, policies and low-level security configurations. In this setting, errors are inevitable due to high system complexity and constant changes in requirements, policies and regulations as well as configurations. The PoSecCo project deals with this complexity by establishing a traceable and sustainable link between requirements and configuration settings in the system.

Innovation Achievements

The traceable link enabled by PoSecCo includes two key artifacts:

- The PoSecCo models representing functional elements of IT systems and corresponding models of security-relevant information for each of these elements. The PoSecCo model repository can be further extended with new models suitable for different kinds of policies and technologies.
- The PoSecCo integrated prototype that smoothly consolidates different prototypes developed in the project. The integrated prototype includes the central model repository (the MoVE tool), a collaborative system for eliciting security requirements and high-level policies monitoring (the CoSeRMaS system), a tool for policies specification and conflict resolution (the IT Policy tool), a decision support system for security (SDSS), and tools for audit support and configuration validation.

Market acceptance gaps

An organization that wishes to adopt the PoSecCo technology has to invest into the collection of information required for creating a functional model of its IT system.

Mitigation strategies

For organizations that already have models or diagrams of their systems and security settings, the up-front investment in the PoSecCo technology can be relatively small, but for unprepared companies the required investment might be significant. An example of technology that is required by PoSecCo is a configuration management database.

PoSecCo further more allows extending and specializing its policy models for other security-domains than authorization, authentication and communication protection (e.g., data protection model).

Impact

The PoSecCo approach allows organizations to manage consistently their high-level requirements and low-level software system configuration and to ensure compliance with existing laws and regulations.

Zoom in

The integrated prototype is evaluated with respect to its appeal to the end-users. The project has conducted a prototype evaluation study with real users of the prototypes, e.g. security analysts, system administrators and compliance managers in the companies that are part of

the PoSecCo consortium. The project has also identified performance indicators for the tools and is going to measure the prototype usage with respect to these key metrics.
The models are validated as a part of the tools; PoSecCo also tries to reach out to interested researchers and policy providers and get their feedback regarding the models.

Have a look at

The PoSecCo tools are available at the project webpage. After the project will finish the demonstration platform of the integrated PoSecCo prototype will be available at least for one more year to allow researchers and practitioners to experience PoSecCo.

SYSSEC

Acronym	SysSec
Project	A European Network of Excellence in Managing Threats and Vulnerabilities in the Future Internet: Europe for the World
Dates	2010-09-01 to 2014-08-31
Participants Number	8
Coordinator	FORTH-ICS Greece
Other participants	Polytechnic University of Milan Italy, The Vrije University of Amsterdam Netherlands, EURECOM France, Vienna Technical University Austria, Chalmers University of Technology Sweden, UEKAE at TUBITAK Turkey, IICT-BAS Bulgaria
Website	http://www.syssec-project.eu
Classification in CORDIS	Trustworthy Network Infrastructures, Future Internet

Objectives

SysSec is a Network of Excellence in the field of systems security in the European Union. Its main goals are to promote cybersecurity education, create a research roadmap, identify threats and vulnerabilities of the Future Internet, and support collaborations among EU research organizations.

Innovation Achievements

One of the research directions of SysSec is mobile security threats, with Vienna University of Technology as the responsible partner. The innovative results produced in this stream focus on dynamic mobile malware detection.

Andrubis is a dynamic analysis environment for Android applications produced within the project. This environment provides a publicly available submission interface for security researchers and average mobile users alike.

Among other achievements of SysSec are:

- An EU systems security research roadmap.
- A common curriculum in security for EU universities.

Market acceptance gaps

The project sees high engagement from end-users; there are already more than 200,000 submissions. Potential threats for acceptance that the project sees come from the academia-driven environment, where each implementation is typically carried out by students. In this way it is difficult to maintain the prototype after the student has graduated and it is almost impossible to have an implementation mature enough to become a real product.

Mitigation strategies

The project continues to improve the prototype by constantly adding features; there are always several students involved to ensure continuous maintenance.

Impact

Android malware is on the tremendous rise, with almost exponential growth in malware samples number over 2012. Availability of free and user-friendly tools to cross-check applications is quite important in this setting.

The impact of the main SysSec activities (the roadmap and the security curriculum) will be quite significant. The security field is relatively new, and the skills gap reported by many project leaders is already present. This skills gap may be overcome by introducing new comprehensive security courses in the standard EU university curriculum.

Zoom in

One of the highlights during 2012 was the first SysSec summer school. The interest in the summer school was very high and well beyond the project expectations. The topic of the school was system security and malware reverse engineering with a special focus on critical infrastructure protection.

A hands-on approach was taken to teach reverse-engineering of malware, especially looking at the recent threats targeting critical infrastructure. One of the core goals of the SysSec

project is promoting cyber security education, by creating a curriculum as well as organizing and collecting material that can be used by teachers across Europe to educate the next generation of researchers and industrial practitioners. For that reason the project has compiled the material from the summer school to be shared with associate partners through the SysSec Course Repository. Associate membership with SysSec is open to any researcher or practitioner.

Have a look at

Play with Andrubis: the dynamic malware analyzer produced by SysSec. You can find the details how to submit applications at http://analysis.iseclab.org SysSec validates its malware analyzer by comparing the results with known malware samples analyzed manually. The analysis results are available at the Andrubis website.

In September 2013 SysSec delivers The Red Book: A Roadmap for Systems Security Research. Contact the project for it.

TAMPRES

Acronym	TAMPRES
Project	TAMper Resistant Sensor node
Dates	2010-10-01 to 2013-09-30
Participants Number	8
Coordinator	IHP Innovations for High Performance Microelectronics, Germany
Other participants	NXP Semiconductors Belgium, NXP Semiconductors Germany, Catholic University of Louvain Belgium, France Telecom, ETH Switzerland, Graz University of Technology Austria, Coalesenses Germany
Website	http://www.tampres.eu/
Classification in CORDIS	Trustworthy Network Infrastructure, Future Internet

Objectives

TAMPRES works on security mechanisms for microcontrollers hardware that will be used in various devices in the Internet of Things (IoT). IoT envisions integration of computing devices and physical world into a seamless global communication network. Specific focus of TAMPRES is on wireless sensor nodes that are likely to become the most vulnerable part in the chain of trust. The nodes therefore need to be protected at the physical level against attacks on their security mechanisms; yet the novel protection mechanisms have to be low cost.

Innovation achievements

The TAMPRES methodology follows an attack-driven approach. Starting from identifying attacks on existing commercial microcontrollers the project develops hardware mechanisms for protection against these attacks, while taking into account the device constraints, such as energy. The key novel contributions by the project are:

- Secure development process for microcontrollers that enable resistance to physical attacks, fault injection and side-channel attacks.
- A number of security engines, such as cryptographic engines and hashing engines.
- Secure wireless interface for microcontrollers.
- Secure memory mechanism to run attested code.
- The attack-resistant TAMPRES architecture that integrates securely all developed components, including protected interfaces for testing and debugging, a secure bootstrapping capability and lightweight memory protection.

Market acceptance gaps

Currently there are no existing alternatives to TAMPRES secure devices; therefore the market for them is not yet developed.

Mitigation strategies

The project engages into various activities to promote its results and open up the market. In July 2013 TAMPRES has conducted a workshop with potential customers to present the project solutions.

The NXP partner in the TAMPRES consortium will adopt some of the developed solutions in their chips.

Impact

TAMPRES secures microcontroller chips for wireless sensor networks in a holistic way yet taking into account cost-effectiveness. The technology can be immediately accepted by end-consumers.

Zoom In

The developed secure components are tested using AFPG designs. The integrated prototype of a secure microcontroller is implemented on an ASIC chip.

Notice that TAMPRES comprises the leading industry partners in chip hardware security. The partners have already acquired four patents for their technology.

Have a look at

The paper “Fast multi-precision multiplication for public-key cryptography on embedded Microprocessors” by Michael Hutter and Erich Wenger was awarded with the Best Paper Award at the 14th Workshop on Cryptographic Hardware and Embedded Systems 2011 (CHES 2011).

UTRUSTIT

Acronym	uTRUSTit
Project	Usable TRUST in the Internet of Things
Dates	2010-09-01 to 2013-08-31
Participants Number	6
Coordinator	CURE Austria
Other participants	Sweden Connectivity Sweden, Search-Lab Hungary, Technical University of Chemnitz Germany, Norsk Regnesentral Norway, Catholic University of Leuven Belgium
Website	http://utrustit.cure.at
Classification in CORDIS	Mobile Devices and Smartphones, Technology&Tools

Objectives

The UTRUSTIT project focuses on understanding trust in the Internet of Things formed by a variety of interconnected devices that are becoming integrated into everyday objects like washing machines, fridges, medical cabinets and even lamps. The Internet of Things collects a large number of communication and information devices, and with this network it is becoming difficult for the user to keep track of the personal information she shares with those devices and control how this information is propagated across the Internet of Things. UTRUSTIT has aimed at putting the user back in control of these personal data sharing and at providing transparency of what information is being sent, while ensuring usability and compliance with the EU Regulations.

Innovation achievements

UTRUSTIT delivers the following key results:

- 6 Personas: 6 archetypical users representing the diverse target groups of the project ranging from early adopters to technology reacting users as well as elderly users and users with disabilities.
- The Trust Feedback Toolkit (TFT) that enables the user to administer the relevant devices and to get an understanding of their potential to transmit private information.
- A Virtual Environment implementation comprising various devices where users can navigate and interact with the devices. The Virtual Environment is used for evaluation of the project TFT prototype (based on the UTRUSTIT methods for simulation, assessment and evaluation of secure, trustworthy and trusted design).
- An investigation of legal and ethical constraints for the Internet of Things and the TFT.

Market acceptance gaps

The TFT concept is the main marketable result of the project. For it to be adopted by providers of the Internet of Things technology, the providers need to be willing to comply with the transparency principles of the TFT and to provide the TFT access to a dedicated API of their applications.

Mitigation strategies

UTRUSTIT promotes the TFT via Internet navigation procedures and demonstrators, such as a demonstrator of a door locker at a medical cabinet. The project is also in contact with several other research projects working in related fields (e.g. ANIKETOS and TWISNET).

Impact

Availability of the UTRUSTIT TFT framework in the Internet of Things will enable more trustworthy and secure infrastructure for all end-users. The results of the validation activities conducted by UTRUSTIT with real end-users and the body of knowledge regarding legal, ethical and usability requirements compliance in the Internet of Things can be used by policy makers, enterprises and research organizations active in the area.

Zoom In

The project has run three use cases: a smart home environment, a smart office and an e-voting scenario. The Virtual Environment created in the project was built for the smart home and smart office scenarios and was used to simulate the interactions of real end-users with

the target devices. More than 60 users took part in the validation activities, with their feedback continuously feedback to the prototype design and implementation. The e-voting scenario was used to evaluate the legal concerns underlying the scenarios.

Have a look at

The article by the UTRUSTIT participants J. Dumortier and N.Vandezande “Trust in the Proposed EU Regulation on Trust Services” was published in Computer Law & Security Review, vol. 28(5), 2012.

Call 8

Project Presentation Outline

For the projects of Call 8, similarly to Call 5, we present the following details. For each project we present a short summary details from CORDIS, a summary of project objectives in comparison with the state of the art and the key innovative contributions that the project strives to achieve. We review potential technology acceptance gaps foreseen by the project and the mitigation strategies that are executed. We then summarize potential impacts from the project on technology, standards, security laws, policies and society in general, and zoom in the validation and dissemination activities run by the projects. For each project we also point the interested readers to some latest news&events.

The presented information is based on personal interviews conducted by UNITN with the projects' leaders. The next projects are overviewed in this section:

- A4CLOUD
- ATTPS
- EURO-MILS
- FUTUREID
- HINT
- INTER-TRUST
- MUSES
- NEMESYS
- RASEN
- TRESCCA
- TRESPASS

The next projects are not reported in this section:

- ACDC
- CIRRUS
- CUMULUS
- CYSPA
- D-MILS
- FIRE
- OPTET
- STANCE
- SECCORD
- STREWS

More details about the projects listed above are available in the CORDIS system [1].

A4CLOUD

Acronym	A4CLOUD
Project	Accountability For Cloud and Other Future Internet Services
Dates	2012-10-01 to 2016-03-31
Participants Number	13
Coordinator	HP UK
Other participants	Athens Technology Centre (ATC) Greece, Cloud Security Alliance Europe UK, ARMINES France, EURECOM France, Furtwangen University Germany, Karlstad University Sweden, Queen Mary University of London UK, SAP Germany, University of Malaga Spain, SINTEF Norway, Tilburg University Netherlands, University of Stavanger Norway
Website	http://www.a4cloud.eu
Classification in CORDIS	Cloud Security

Objectives

Accountability is central to a trustworthy cloud – an accountable cloud ecosystem is necessary for innovation and growth ambitions. Accountable organisations ensure that obligations to protect data are observed by all who store and process the data, irrespective of where that processing occurs. Without accountability, cloud consumers will lack confidence to put personal data (and any other confidential data) in the cloud. Cloud consumers want to be confident that service providers are treating data appropriately and that they can retain control over how it is used, that the legal frameworks are effective, and that they have ways to hold providers accountable for what happens to that data. Cloud providers need a way to implement accountable cloud services.

Innovation targets

A4CLOUD produces its results with respect to four perspectives: technical, legal, socio-economic and ethical. With these perspectives in mind, the project will develop the following innovations:

- A framework for accountability in the cloud that includes concrete practical definitions of accountability and its attributes to be implemented, practices to be followed and tools to be deployed for an organization to be accountable.
- A toolset for accountability including preventive, corrective and detective modules. The modules will be suitable for monitoring data handling, ensuring its compliance with user expectations, organization policies and regulations and identifying potential risks of compliance violations.
- An architecture for accountability and best practices that can be implemented by an organization.

Market acceptance gaps

Cloud service providers are a community of practice, they typically operate based on common practices and established guidelines. For the project to be successful it has to promote its technology so that it becomes a de-facto practice in the community. During the first year A4CLOUD will promote its concepts of accountability and discuss elicited accountability requirements. In the second year the project will promote the framework and tools it designs. Finally, during the last year the project will disseminate practices and procedures for accountability.

Mitigation strategies

The Cloud Security Alliance is the partner mainly responsible for engagement with the cloud service providers' community. HP has already engaged its internal Privacy&Compliance Office in adoption of the project results.

Impact

With the A4CLOUD accountability framework deployed end-users of cloud services will be in control of their data. For organizations it will be simpler and less costly to implement the data protecting regulations, assess risks and monitor compliance.

Zoom in

A4Cloud promotes an accountability-based approach for cloud services supporting three different aspects of data governance; those that are *preventive* (for example mitigating risk, and to certain extent, policy enforcement), *detective* approaches (such as monitoring and identifying risk and policy violation) and *corrective* techniques (managing incidents and providing redress).

Have a look at

A4CLOUD has issued a white paper “Conceptual Accountability Framework”. Contact the project for it.

ATTPS

Acronym	ATTPS
Project	Achieving The Trust Paradigm Shift
Dates	2012-07-01 to 2015-06-30
Participants Number	9
Coordinator	BICORE, Netherlands
Other participants	Thales Communications&Security France, KTH Sweden, Nokia Finland, NEC UK, Gemalto France, Technical University of Berlin Germany, Philips Electronics Netherlands, EIT ICT Labs Belgium
Website	Dedicated website is not available http://www.trustindigitallife.eu
Classification in CORDIS	Networking, Coordination and Support

Objectives

The ATTPS project exists under the umbrella of the Trust in Digital Life (TDL) initiative; it is one of supporting actions of this initiative. ATTPS aims at enabling a trust paradigm shift in the community. Currently people sometimes do not realize that free services they use are actually trading their data with third parties. ATTPS strives for promoting awareness that trustworthy solutions that do not disclose user data to third parties can be rarely available for free. The project also works on an experimental platform for validating trustworthiness of Internet solutions.

Innovation targets

ATTPS will work on promotion of public debates regarding the trust paradigm shift and on raising awareness in the community; it will also analyze and address business, legal and social challenges of the paradigm shift.

On the technical side the innovation goals are:

- The ATTPS validation environment including testbeds and secure components developed by the members of ATTPS and TDL, such as secure 3G network and secure authentication mechanisms. This environment can be explored by organizations to analyze trustworthiness and acceptability of their services. The environment can be used either with support of a usability lab or a Living Lab with actual end-users.
- Generic trust architectures for mobile and service platform integrity, and secure data lifecycle management.

Market acceptance gaps

ATTPS does not see any particular market acceptance gaps because it is an industry-driven project, and their contributions are requested by the industrial partners in the project and other organizations affiliated with TDL. A potential threat for ATTPS could be the acceptance by the industry outside of the TDL community.

Mitigation strategies

The project's main players are industry partners that work closely with research organizations on validation of their solutions. ATTPS is also tightly integrated with the TDL community that includes big industry players, such as SAP and Microsoft. The project interacts with all members of TDL, and builds its architectural solutions and validation platform components on these interactions.

Impact

ATTPS expects to have a wide impact on the community. As a result of its activities the project envisions changes to common understanding of trust in the Internet and changes to the trustworthiness and interoperability of the EU services. The project is also engaged in standardization activities and interacts with legislation and law enforcement authorities on the EU level and on national levels.

Zoom in

The project has a demonstrator that shows to a user the value of her data provided on the Internet; it works by gathering the shared information and evaluating which companies are making money with it. ATTPS also works on promoting privacy awareness in an app store by notifying the users how well an app deals with their private data. The project monitors whether people are actually influenced by this indicator with shopping for apps.

Have a look at

The Trust in Digital Life consortium has produced Strategic Research Agenda for Trustworthy ICT that includes roadmaps for R&D progress towards Horizon 2020 and overviews challenges to overcome. The Agenda can be found at the consortium's website http://www.trustindigitallife.eu.

EURO-MILS

Acronym	EURO-MILS
Project	Secure European Virtualization for Trustworthy Applications in Critical Domains
Dates	2012-10-01 to 2015-09-30
Participants Number	14
Coordinator	TECHNIKON Austria
Other participants	Airbus France, T-Systems Germany, SYSGO Germany, SYSGO France, Open University of the Netherlands, University Paris-Sud France, EADS Germany, EADS France, Thales Communications&Security France, University of Gent Belgium, German Center for Artificial Intelligence Germany, OPENSYNERGY Germany, Jemm Research France
Website	http://www.euromils.eu
Classification in CORDIS	Technology&Tools

Objectives

EURO-MILS focuses on high-assurance certification using the Common Criteria standard for security evaluation of highly critical embedded systems based on the MILS (Multiple Independent Levels of Security) approach. Cyber-physical networks of embedded systems are becoming widespread today, with such examples as cars or aircrafts interconnected with their manufacturer, operation companies and public networks. Such systems include components with high security demands while being connected to the Internet. Therefore, there is a demand for strong security and reliability guarantees for these systems. The EURO-MILS project will work on providing trustworthiness by design and high assurance for such systems, including strong isolation guarantees for resource sharing, by means of security certification.

Innovation Targets

The EURO-MILS main innovative targets are:

- The first certification in Europe of a separation kernel, one of the main components of a MILS system according to a Common Criteria Security Target.
- Development of a MILS architecture-based design for MILS systems that will offer secure virtualization of complex systems into independent components with tight control of information flow among them. The design is suitable to achieve security certification (according to the Common Criteria standards) and verification with formal methods supporting the main components to build a MILS system.
- Proof-of-concept prototypes for the project use cases in the avionics and automotive domains.

Market acceptance gaps

EURO-MILS partners put major efforts in analyzing the current market by having a special work package on business, legal and social acceptance, lead by a market analysis expert organization (Jemm Research). Within that work package, all business and market aspects will be analyzed.

Generally, it can be said that the adoption of the EURO-MILS technology may be hindered by lack of acceptance by the industry, if they do not believe that the MILS architecture approach achieves sufficient security levels. Another important aspect required by the industry is cost-effectiveness.

Mitigation strategies

The project will deliver the main components to build a MILS system proven to be secure by the Common Criteria security certification. EURO-MILS analyses the business impact of trustworthy ICT for networked high-criticality systems and is working of a low-cost implementation of the technology to address the cost-effectiveness.

Some of the EURO-MILS consortium partners are experts in Common Criteria certification (DFKI, T-Systems and Thales), which guarantees a very professional approach and therefore a high level of confidence that the industry would accept the solution.
The consortium partners, such as Airbus and OpenSynergy, have plans to adopt the project results into a multitude of applications.

Impact

The architectural approach, which is validated by certification and prototypes that is delivered by EURO-MILS will bring more security and trust into critical embedded systems. The project's Advisory Board consists of governmental security authorities, to strengthen the highly strategic importance for Europe.

Zoom in

The project relies on industrial validation of its results. It has two use cases:

- An aircraft steering system (by Airbus and EADS)
- An automotive combined infotainment and connectivity system (by OpenSynergy)

The baseline technology provided by SYSGO is already certified according to high levels of safety in e.g. the avionics and railway sector and therefore already covers one part of the trustworthiness paradigm (the other being security as defined by the Common Criteria).

Have a look at

The EURO-MILS homepage presents the latest news about conferences, workshops and meetings organized by the project (such as the EURO-MILS Workshop on MILS Architectures and Components held in August 2013) as well as recent publications and deliverables: https://www.euromils.eu/

FUTUREID

Acronym	FutureID
Project	Shaping the future of electronic identity
Dates	2012-11-01 to 2015-10-31
Participants Number	19
Coordinator	FIT at Fraunhofer, Germany
Other participants	SK Estonia, University of Stuttgart Germany, Catholic University of Leuven, AGETO Germany, Graz University of Technology Austria, Norsk Regnesentral Norway, University of Newcastle upon Tyne UK, Gemalto France, Giesecke&Devrient Germany, Comarch Poland, Infineon Technologies Germany, Technical University of Denmark, IBM Research Switzerland, Technical University of Darmstadt Germany, EEMA Belgium, ULD Germany, ATOS Spain
Website	http://www.futureid.eu
Classification in CORDIS	Privacy Management

Objectives

The FutureID project focuses on interoperability of electronic identification (eID) systems. The existing European eID technologies are often not compatible, with each identity provider issuing its own credentials unrecognizable by other providers. FutureID wants to build a comprehensive, flexible, privacy-friendly but also usable identity management infrastructure for Europe, which will integrate existing eID solutions and trust infrastructures.

Innovation Targets

The FutureID infrastructure will comprise the following innovative technologies:

- The Identity Broker technology that is a domain middleware or a back-end component to guide the user to the right identity scheme. The brokers will become bridges between service providers and relying parties on one side, end-users on the second side and identity providers on the third side. The user will be empowered with the possibility to choose which credentials he would like to use.
- An open source eID client implementing the FutureID technology, which is capable of running on multiple different platforms.
- An application integration service for relying parties to ease integration of existing services into the FutureID infrastructure.

Market acceptance gaps

The FutureID infrastructure will be a success only if service providers accept it for accessing their services. Since the end-users are involved, the framework also needs to be easy to use and economically viable for the users.

Mitigation strategies

The project works on attracting service providers by enabling the application integration service that makes the integrated eID infrastructure cost-effective and easy to handle for the service providers.

With respect to the end-users FutureID conducts extensive usability assessments of its technologies and studies to discover the end-user preferences and willingness to pay for the eID solutions. The project works on fitting the infrastructure to the current market demands.

Impact

The FutureID infrastructure will provide benefits to all stakeholders involved in the eID value chain. End-users will benefit from the availability of an open source eID client that is capable of running on an arbitrary platform. Service providers will be able to integrate their existing services with the FutureID infrastructure without substantial investments. For trust service providers FutureID will ease usage of their authentication- and signature-related products across Europe and beyond.

Zoom in

To demonstrate feasibility of the infrastructure FutureID will develop two pilot applications:

- A public service-oriented pilot applications run in collaboration with the epSOS project;
- A business-oriented service marketplace use case (by Atos).

An independent evaluation work package will continuously assess whether the FutureID project meets the technical, social, economical and legal requirements elicited in the beginning of the project.

Have a look at

After the first year the project will produce deliverables on the requirements elicited and business use cases for the FutureID framework. Retrieve them at the project website.

HINT

Acronym	HINT
Project	Holistic Approaches for Integrity of ICT-Systems
Dates	2012-10-01 to 2015-09-30
Participants Number	7
Coordinator	TECHNIKON Austria
Other participants	Infineon Technologies Austria, Catholic University of Leuven Belgium, CEA-LETI France, ARMINES France, Cassidian Cybersecurity France, Morpho Cards Germany
Website	http://www.hint-project.eu
Classification in CORDIS	Trustworthy Network Infrastructures

Objectives

HINT strives to design and implement a common framework for system integrity checking based on the trusted computing technology. Integrity is becoming a predominant issue for integrated circuits (chips) used e.g. in critical embedded systems and smart cards, because the hardware that executes sensitive primitives needs to be trustworthy. HINT operates with hardware-software interweaving and devises new techniques to ensure the chip is genuine and its integrity is preserved.

Innovation Targets

The HINT framework for integrity checking will include the next key innovations:

- A novel integrity checking technology based on the side-channel analysis, which will become one of the first practical applications of the side-channel analysis to ensure security instead of breaking security.
- Energy-optimized nanostructures for integrity that will allow for checking the genuineness of hardware at moderate cost level.
- Two integrated proof-of-concept prototypes to demonstrate the HINT technology.

Market acceptance gaps

The HINT technology acceptance could be hindered due to its costs, because cost-effectiveness is one of the major requirements of the domain.

Mitigation strategies

The project works on economically viable solutions from the start, driven by the leading industrial players in the integrated circuit production in Europe. The industrial partners (Infineon, Cassidian CyberSecurity and Morpho) have elicited the security requirements for mass-market prototypes. HINT foresees wide adoption of its technology in mass-market chips, possibly in the near future.

Impact

HINT addresses several legislative actions taken by the European Commission to check integrity and hardware trustworthiness. If the project achieves its ambitious goals the overall security of integrated circuits will be improved, enabling higher security of end-user devices.

Zoom in

One mission of HINT is to prepare the adoption of the proposed technologies by future Common Criteria evaluation schemes.

Have a look at

The HINT homepage (http://www.hint-project.eu) contains news about conferences, workshops and meetings as well as latest publications and deliverables.

A recent paper by the HINT consortium members appeared at IEEE International Symposium on Hardware-Oriented Security and Trust (HOST'2013). Discover the paper "Side channel modeling attacks on 65nm Arbiter PUFs exploiting CMOS device noise" by J. Delvaux, and I. Verbauwhede at http://www.hint-project.eu/index.php/publications

INTER-TRUST

Acronym	INTER-TRUST
Project	Interoperable Trust Assurance Infrastructure
Dates	2012-11-01 to 2015-04-30
Participants Number	11
Coordinator	Softeco Sismat Italy
Other participants	Montimage France, Telecom Bretagne France, Telecom SudParis France, University Rovira I Virgili Spain, Search-Lab Hungary, University of Malaga Spin, University of Reading UK, University of Murcia spain, SCYTL Spain, INDRA Spain
Website	http://inter-trust.lcc.uma.es or http://www.inter-trust.eu
Classification in CORDIS	Networking, Coordination&Support, Technology&Tools

Objectives

INTER-TRUST focuses on security in service environments. Service-oriented Architectures (SOA) today lack the means to verify trustworthiness of individual services or service compositions, while they rely extensively on constant interactions of dynamically evolving services. INTER-TRUST investigates the means to bring security and compliance with legal, social and economics requirements to SOA.

Innovation Targets

The project works to develop the following main innovations:

- A conceptual INTER-TRUST framework for trust and security policies negotiation among composite services and dynamic introduction of security features to existing software without fully rewriting the code.
- An INTER-TRUST prototype serving as a complete proof-of-concept implementation of the conceptual framework.

Market acceptance gaps

The project's goals are quite ambitious and it is not yet clear whether it will be possible to achieve all targets within the timeframe of INTER-TRUST. Even if all challenges are resolved, at this stage it is not yet clear how to market and monetize the project's results as commercial products.

Mitigation strategies

The project has developed a gradual approach to tackle challenges in order to ensure at least partial successful results are obtained. The marketing strategy and conversion to commercialization of the INTER-TRUST technology are currently under investigation by the project, and the partners intend to carry on the market exploitation even after the project finishes. The first potential customers of the INTER-TRUST products are already within the project consortium, as the use case providers are quite interested in adoption of the project results.

Impact

The INTER-TRUST project can bring affordable security technology for services that can be used also by SMEs. The consortium is already in contact with a number of SMEs and it receives their feedback regarding the proposed solutions.

Zoom in

The project has two use cases to try out its technology: an electronic voting system, and an intelligent transportation system with vehicle-to-vehicle and centralized communications capabilities.

Have a look at

The project has published a Deliverable 2.5.1 Legal, Social and Economical Constraints Specification (V1). The deliverable collects legal, social and economic requirements and constrains related to the INTER-TRUST framework, with an emphasis on the interests of the main industrial actors, e-voting, and traffic and transport co-operative services. Obtain the deliverable at the project website.

MUSES

Acronym	MUSES
Project	Multiplatform Usable Endpoint Security
Dates	2012-10-01 to 2015-09-30
Participants Number	9
Coordinator	S2 Grupo Spain
Other participants	University of Granada Spain, HITeC at the University of Hamburg Germany, Catholic University of Leuven Belgium, CURE Austria, Sweden Connectivity Sweden, WIND Italy, University of Geneve Switzerland, TXT e-Solutions Italy
Website	https://www.musesproject.eu/Muses
Classification in CORDIS	Technology&Tools

Objectives

The MUSES project can be summarized in three words as Usable Corporate Security. Employees of organizations typically have access to sensitive corporate data but they often lack expertise to deal with these data in a secure way. The security practitioners have discovered some time ago that end-users are often the weakest link due to common lack of awareness or even malicious intentions. Moreover, the Bring Your Own Device (BYOD) practice, when employees are allowed to use untrusted private devices for work, is becoming quite common in large organizations and posing new threats to corporate security. MUSES aims to provide a system to enforce corporate security policies while taking into account such challenges as information delocalization, end-user privacy, mixing of private and corporate activities on a single device and usability.

Innovation Targets

The project will deliver a device-independent, user-centric and self-adaptive corporate security framework to deploy and enforce corporate security policies. The framework will combine the following innovative features:

- A device-agnostic technique to deploy and enforce corporate ICT security policies.
- A technique to detect anomalies in the user behavior while not intruding upon the user privacy and in compliance with existing EU and national laws.
- An open source prototype of the MUSES framework that will allow BYOD security. The framework has to be self-adaptable in order to be able to incorporate changes to the policies, regulations and laws and the hosting platform modifications.

Market acceptance gaps

An important aspect of viability of the MUSES platform is its usability and acceptance by the end-users. If end-users are concerned that they are monitored while working with their own device (as in the BYOD setting), they might feel offended and could try to switch the monitoring off, effectively disabling the security protection.

The MUSES solution has to be easily transferrable to new versions of computing platforms (e.g. new versions of Android or iOS) due to the variety of platforms existing today and fast evolution of the market.

Mitigation strategies

The project consortium includes usability experts, legal experts and privacy experts to work on gaining the end-user acceptance. MUSES also plans to deploy its platform to real end-users and receive feedback from potential customers from early stages of the project.

To ensure that the MUSES platform can be transferred from one platform to another the project considers two approaches: to enhance the platform self-adaptability so that it can adapt to any changes to the operating system, or to convince the platform owners to include MUSES into the platform distributions.

Impact

Organizations through deployment of the MUSES platform will be able to enhance corporate security and reduce costs of security incidents and device ownership (by adopting the BYOD paradigm). The end-users will have more trust in their devices and services they access.

Zoom in

The project will run two trial studies with end-users to evaluate the prototype in the corporate environment. The responsible partners are TXT e-Solutions and WIND.

Have a look at

The project has published a survey of trust and risk metrics to assess user computing environments. Retrieve it from the project website

https://www.musesproject.eu/Muses/publication/deliverables/d3.1-survey-of-trust-and-risk-metrics-to-assess-user-computing-environments/view

NEMESYS

Acronym	NEMESYS
Project	Enhanced Network Security for Seamless Service Provisioning in the Smart Mobile Ecosystem
Dates	2012-11-01 to 2015-10-31
Participants Number	6
Coordinator	Imperial College London UK
Other participants	CERTH Greece, COSMOTE Greece, Hispasec Spain, Telecom Italia Italy, Technical University of Berlin Germany
Website	http://www.nemesys-project.eu/nemesys/
Classification in CORDIS	Mobile Devices and Smartphones

Objectives

The NEMESYS project addresses security of mobile devices and networks. These systems are very vulnerable because they move around in uncontrolled wireless mobile network environments. These environments may try to attack mobile devices in attempts to capture some aspects of mobile user identities or to exploit the devices. The NEMESYS aims to analyse the vulnerabilities of mobile devices and to propose mechanisms for detection and protection against attackers exploiting these vulnerabilities.

Innovation Targets

NEMESYS will work on the next innovative contributions:

- Collection of threats of existing smartphone platforms and comprehensive analysis of these threats; including analysis of modus operandi of mobile cybercriminals.
- Virtualized honeypots along with corresponding anomaly detection algorithms produced for several mobile platforms.
- The NEMESYS network data collection infrastructure to collect, detect and provide early warning of attacks on mobile devices.
- The NEMESYS scalable and interactive visualization tools, including and security analytics framework, to provide network traffic and events representation.

Market acceptance gaps

The project envisages that some industrial partners of the consortium may have an incentive to keep the NEMESYS results for themselves instead of turning the results into commercial products.

Mitigation strategies

The project teams up and works closely together to mitigate the risks. Given the highly demanded and competitive nature of the mobile device security domain, the project actively collaborates with potential customers from the start.

Impact

NEMESYS will impact security of individuals and organizations by improving the understanding of novel mobile security threats and cybercriminals exploiting these threats, and providing detection and protection mechanisms against these threats.

Zoom in

The project includes three pipes of activities related to validation that are based on validating real technologies, and not abstract concepts. The first pipe comprises developing use cases together with industrial partners (telecom operators) and validating on these use cases. The second pipe regards a large-scale simulation environment where the validation experiments will be run. The third pipe consists of running experiments in real networks. The project has set up an Ethics Advisor group to ensure the experiments on real networks are ethically acceptable and do not threaten security and privacy of real users.

Have a look at

The first project deliverables surveying state-of-art for security threats and attacks against mobile devices and security controls of existing smartphone platforms are available at the project website.

RASEN

Acronym	RASEN
Project	Compositional Risk Assessment and Security Testing of Networked Systems
Dates	2012-10-01 to 2015-09-30
Participants Number	7
Coordinator	SINTEF Norway
Other participants	Smartesting France, FOCUS of Fraunhofer Germany, EVRY Norway, Software AG Germany, University of Oslo Norway, Info World Romania
Website	http://www.rasen-project.eu
Classification in CORDIS	Trustworthy Service Infrastructures

Objectives

The RASEN project works on techniques for combining two existing security disciplines: risk assessment and security testing. This marriage brings mutual benefits to both fields. Traditional risk assessment is usually done through a series of workshops with experts, and there is always a degree of uncertainty to the information they provide. Security testing, on the other hand, typically requires execution of a huge number of tests and it may not be feasible to cover all of them in a short time. RASEN streamlines interaction between these two fields to allow an organization to have a global view on its security status and improve the results of both disciplines.

Innovation Targets

The project mainly focuses on organizing bi-directional information exchange from risk analysis to security testing and vice-versa. The main expected innovations are:

- The risk-based security testing technique that allows to prioritize security tests to be executed based on the result of risk analysis.
- The test-based risk assessment technique to reduce uncertainty of risk analysis by using results of security testing of the system.
- The legal security risk assessment methodology, which will be used by organizations to show that software systems they develop are compliant with existing laws and regulations.
- A compositional risk assessment methodology to allow execution of risk assessment on large-scale systems in a modular way.

Market acceptance gaps

RASEN will deliver prototype tools for its methodologies. Yet the project foresees potential gaps for adoption of its results in the absence of industrial-level tools that are required by practitioners.

Mitigation strategies

As part of the RASEN prototype toolbox, the project will develop a self-contained core subset which will be sufficiently mature to enable ease of adoption.

Impact

The results of RASEN will help organizations to conduct security assessments of large-scale information systems through the combination of security risk assessment and security testing, taking into account also the context in which the system is used, such as liability and legal dimensions.

Zoom in

The use cases explored by RASEN are:

- A healthcare system use case with a strong focus on compliance with privacy regulations (by Info World).
- A financial software system use case with a focus on test prioritization and compliance with regulations regarding financial systems (by EVRY).
- A business process software system use case with a focus on scalability (by Software AG)

Have a look at

In November 2013 RASEN co-organizes the Workshop on Risk Assessment and Risk-driven Testing (RISK'2013). Check out the workshop website at

http://www.fokus.fraunhofer.de/en/fokus_events/motion/risk_2013/index.html

TRESCCA

Acronym	TRESCCA
Project	TRustworthy Embedded systems for Secure Cloud Computing Applications
Dates	2012-10-01 to 2015-09-30
Participants Number	7
Coordinator	OFFIS Germany
Other participants	CoSynth Germany, Wellness Telecom Spain, VOSYS France, Technological Educational Institute of Crete Greece, ST Microelectronics France, Telecom ParisTech France
Website	http://www.trescca.eu
Classification in CORDIS	Cloud Security, Mobile Devices and Smartphones

Objectives

TRESCCA addresses security and trustworthiness of cloud platforms. Today cloud service providers and their end-users do not always trust each other. The classical cryptography can be an efficient solution for cloud storage systems. Yet remote processing of sensitive data or cloud computations on sensitive data require users to give full access to the data to the cloud service providers; and currently they sometimes do not want to do this due to lack of a strong chain of trust. This chain of trust between the cloud operators and the end-users is the main goal of the TRESCCA project.

Innovation Targets

TRESCCA focuses on entanglement of hardware and software security techniques in order to achieve the following key breakthroughs:

- A secure client platform that will be able to securely process the sensitive data in a fully transparent manner. In the TRESCCA concept the user data will be only stored locally, while the cloud service providers will outsource to the secure and trusted platform of the user the computation primitives they want to perform with the user data.
- A prototype implementation (both hardware and software components) of the secure client. The prototype will be comparable to a set-top box and it will be possible to use it in a home environment.
- An ecosystem for the secure client: APIs to use the client features and implement applications for it, and APIs to interact with the client from the cloud side.
- An approach to securely migrate virtual machines from one platform to another (as a crucial part of the secure client)

Market acceptance gaps

The project is convinced they can attract customers if all ambitious goals of the project can be achieved. However, most of the project results will be open to interested parties, therefore the project envisages they can offer to the customers expertise in adopting the TRESCCA technologies to other platforms, rather than selling the final integrated prototype as a product.

Mitigation strategies

TRESCCA constantly interacts with players from different industry domains through its Advisory Board, which comprises, among all partners, legal advisors in the domain of Internet security. The feedback from the Advisory Board is used to navigate the project following the latest industry trends and demands.

Impact

Availability of the TRESCCA secure client will allow cloud service providers and their end-users to have mutual trust. The end-users will have full control over their sensitive data, while service provider will remain assured that the computations are performed correctly. The core technologies devised by TRESCCA (hardware security modules enhancements, secure virtualization, virtual machine migration, etc.) will benefit to security of devices in other domains.

Zoom in

TRESCCA runs three use cases to evaluate its solutions: digital rights management in a home environment, smart metering-as-a-service, and a generic authentication component for the TRESCCA client.

Have a look at

One of the biggest challenges ahead of TRESCCA is live migration of virtual machines. The secure client requires portability: the ability to migrate an application and its state from one platform to another platform. Yet the differences of the platforms are immense, as they have different hardware and different hypervisors. From the current state-of-art point of view it can be compared with trying to play a vinyl on a CD-player. Find out more details of how TRESCCA addresses this challenge at the project website: http://www.trescca.eu/index.php/2013-05-23-13-18-38/live-migration.html

TRESPASS

Acronym	TREsPASS
Project	Technology-supported Risk Estimation by Predictive Assessment of Socio-technical Security
Dates	2012-11-01 to 2016-10-31
Participants Number	17
Coordinator	University of Twente, Netherlands
Other participants	University of Luxemburg, Consult Hyperion UK, Deloitte Netherlands, Aalborg University Denmark, BizzDesign Netherlands, Cybernetica Estonia, Delft University of Technology Netherlands, Hamburg University of Technology Germany, IBM Research Switzerland, itrust consulting Luxemburg, Goethe University in Frankfurt Germany, LUST Netherlands, University of London Royal Holloway UK, Technical University of Denmark, GMVIS SKYSOFT Portugal, GMV SGI Spain
Website	http://www.trespass-project.eu
Classification in CORDIS	Technology&Tools

Objectives

The TREsPASS project aims to identify and protect against information security threats and to improve existing risk management methods. Over the last years successful cyberattacks cost the society billions of euros. Yet the state-of-art approach to combat and especially prevent the attacks consists of analysis of information systems by experts and successive brainstorming to identify the risks. This approach lacks consistency, and risks could be identified only if people can conceive them. TREsPASS will deliver an Attack Navigator tool that will be able to automatically predict and prioritize attacks, and evaluate the benefit of possible countermeasures.

Innovation Targets

The project works on the following key innovations:

- The Attack Navigator tool that will be able to provide a map of existing system components and identify potential attack avenues and their impact. It will also be able to evaluate the benefits of countermeasures against the detected vulnerabilities. Based on the Attack Navigator attack trees will be automatically generated.
- The threats identified by the Attack Navigator will be not only technical threats, but also social (social engineering attack opportunities). The security assessment will be conducted from an integral socio-technical security perspective.

Impact

The TREsPASS technology will reduce the number of security incidents in Europe and provide guidelines on better security investments to organizations.

Zoom in

The project will execute three case studies from different domains: a cloud infrastructure with a focus on security technology, the leading partner is IBM Research Switzerland; a telecommunication infrastructure with a focus on security technology and the business model itself (by Goethe University); and remote payment system for the elderly (by Consult Hyperion).

Have a look at

The project consortium consists of not only experts in information security technology, but also includes experts in social sciences, psychology and engineering. Find out the partners expertise at http://www.trespass-project.eu/Partners

Call 8 Overview

While the industrial impact of the projects in Call 1 and Call 5 has been assessed by the EFFECT+ project[2] in the deliverable D2.2 [2], the projects in Call 8 have started just recently. We therefore provide the same analysis of industrial impact for Call 8 as it was done for Call 1 and Call 5.

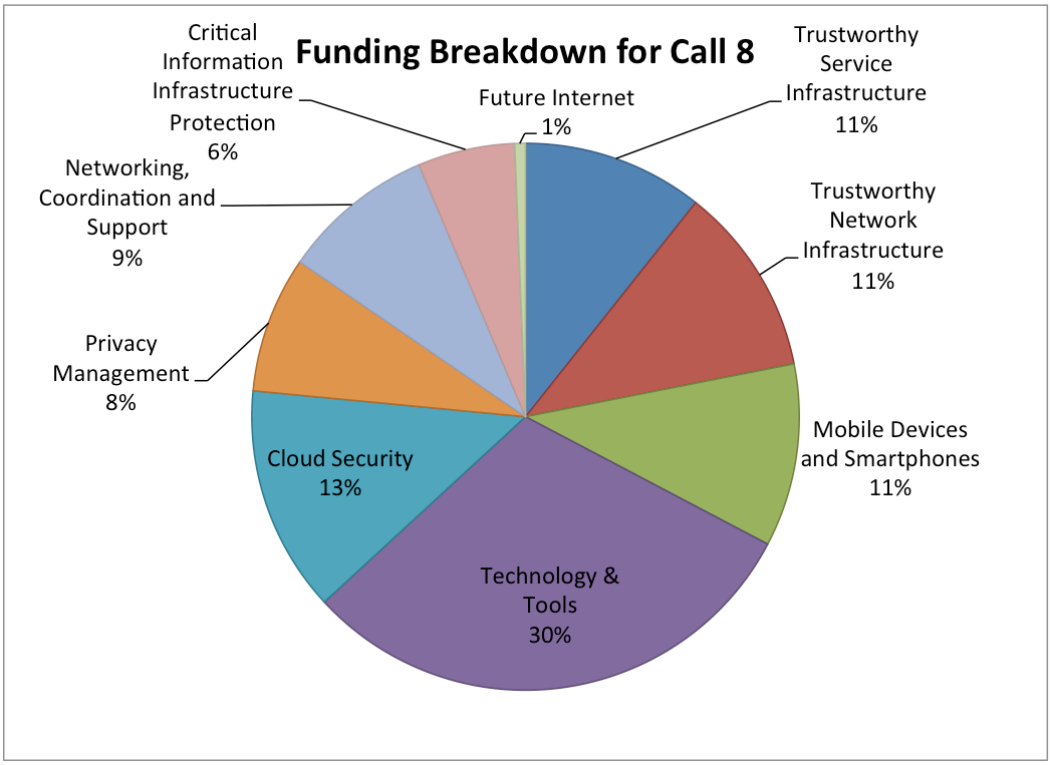

Figure 17. Funding of projects in Call 8 per category

The funding breakdown per CORDIS category in this Call is presented in Figure 17 (again, the projects attributed to several categories appear in all of them). Comparing with the average funding across Calls (in Figure 2) we can notice that Cloud Security; Mobile Devices and Smartphones; and Networking, Coordination and Support are well funded in Call 8, with their funding in Call 8 almost two times bigger than the average across Calls. Also the Technology&Tools category is well funded, acquiring 30% of all funds from the EC. The shares of Trustworthy Service Infrastructures and Future Internet are significantly smaller than the average across Calls.

The funding distribution for the projects of Call 8 confirms that the Cloud Security and Mobile Devices and Smartphones are 'hot topics', where a lot of money is being invested (not only by the EC into R&D projects, but by the industry as well). It will be interesting to see if this trend will continue in Call 10 and if some new categories will appear.

Most projects of Call 8 (those delivering technical results) can be characterized by taking a holistic view on security. They take into account not only technical, but also legal and socio-economic aspects of the technology in question.

Beneficiaries of the Projects' Results

The **ICT Security Industry** comprises companies involved in delivering security technologies. The technologies from the EURO-MILS and D-MILS project for secure virtualization, certification and assurance for critical embedded systems will be of interest for

[2] http://www.effectsplus.eu

this industry, as well as the integrity checking technology for integrated circuits of the HINT project. The software security-oriented companies are direct beneficiaries of the STANCE project that delivers a toolbox for software verification.

The **Telecommunication industry** will be interested in the innovative mobile network threats detection and prevention techniques delivered by the NEMESYS project. Specifically, NEMESYS will work on techniques to protect mobile operators' infrastructures from cyberattacks. The ACDC project will develop techniques to overcome network cybersecurity threats, while the CYSPA project will deliver solutions to prevent disruptions of the Internet infrastructure.

The **domain of ICT Integrators** is interested in techniques to assess organizational risks and ensure compliance with policies and regulations. In this domain the INTER-TRUST framework for ensuring security of composite services will be of interest. The MUSES project will deliver a framework to ensure compliance with the BYOD policies of an organization. In the risk management field the RASEN project will contribute with an entanglement of risk assessment and security testing, allowing an organization to exercise more precise risk assessment and more effective security testing. RASEN will also produce a methodology for legal security risk assessment. The TRESSPASS project will deliver a tool to execute advanced risk management and recommend effective countermeasures automatically.

The **Service Industry** will receive results from a multitude of projects. The **cloud service providers** will be affected by the projects A4CLOUD, TRESCCA, CIRRUS and CUMULUS. A4CLOUD will deliver a framework for accountability of cloud services. TRESCCA will produce a technology to migrate virtual machines from cloud to a user's device and back. The CIRRUS project will dedicate itself to cloud standards and best practices. CUMULUS will offer techniques to certify cloud infrastructures.

The FUTUREID project aims at delivering a cross-platform identity management framework, which the service providers will be able to use to simplify identification of end-users. The ATTPS project will offer a validation environment that service providers can use to evaluate acceptability of their products by end-users. Finally, OPTET will offer technologies to enable evidence-based trustworthiness management for socio-technical Internet-based systems.

Several projects do not aim at providing technical results for a specific industry: FIRE will work on pan-EU roadmapping of Trustworthy ICT research, STREWS will dedicate itself to roadmapping Web security. SECCORD will work on the EU Trust & Security projects clustering.

Such industries as the **General Security industry**, and the **Energy Sector** are not targeted by the projects in this Call.

Trust & Security Programme Analysis

Successes and Gaps in Addressing the Work Programmes' Goals

The main target objectives for Call 1, Call 5 and Call 8 from the respective Work Programmes were presented in Table 1. Let us now overview the extended descriptions of the objectives and map the projects' contributions to the descriptions.
Table 6, Table 7, Table 8 map the objectives of, respectively, Call 1, Call 5, and Call 8 into the projects from these Calls that have contributed to the objectives (for each project we have chosen the most suitable objective). The tables demonstrate that **the most of the specific objectives were successfully addressed**, except for only a few, reported below:

- We can see that **there are not so many projects addressing coordination with related national or regional programmes** (a part of ICT-2007.1.4, ICT-SEC-2007.1.7, ICT-2009.1.4 and ICT-2011.1.4). In this area we can name the projects INCO-TRUST, BIC and FIRE. Yet these projects have addressed alignment with non-European research programmes, and no project has worked on coordination of national research programmes inside the EU. This gap can be explained by the lack of players that could execute such activities. The CYSPA project in Call 8 aims to review the existing national activities in cybersecurity, but this effort may not be sufficient. Yet, the Proposal for the new EU Cybersecurity Directive requires establishment of the national network and information security strategies in each Member State. Therefore there will be a need to align cybersecurity strategies and research initiatives for the EU Member States.
- We can also see based on analysis of the project data that the **scalability challenge** (in particular, required as a part of ICT-2009.1.4: Trustworthy Network Infrastructures, ICT-2009-1.4: Trustworthy service Infrastructures and ICT-2011.1.4: Heterogeneous networked, service and computing environments) **was not addressed sufficiently**, as few projects addressing these objectives report that scalability is an inherent part of their solutions.
- For the Call1 objectives, besides the reported issue of coordination with national programmes, the following contributions were missing:
    - The sub-objective ICT-20071.4: Longer term visions and research roadmaps - "*coordination of FP7 projects addressing security, dependability, privacy and related ethical issues across different challenges and objectives of this Work Programme*" was not addressed explicitly by any project of Call 1.
    - The sub-objectives ICT-SEC-2007.1.7: Technology building blocks - "*availability of security forensics*" and "*developing longer term visions and research roadmaps; metrics and benchmarks for comparative evaluation in support of certification and standardization*" were not sufficiently addressed by the selected CI projects.
- For the Call 5 objectives, besides the issues already mentioned, the following contributions were found missing:
    - The sub-objectives ICT-2009.1.4: Networking, coordination and support: - "*economics of security addressing cost-effectiveness and market compliance of security solutions*", "*promoting wide use of standards, certification models and best practices*" and "*legal and societal aspects related to technology development of trustworthy ICT*" were not sufficiently addressed by the selected projects in this category. Notice that the first two of these sub-objectives are addressed in Call 8 by the projects FIRE (studies the market acceptance) and CIRRUS and STREWS (promote standardization, certification and best practices).
- For the Call 8 objectives the following sub-objectives were not covered sufficiently:
    - The sub-objective ICT-2011.1.4: Trust, e-identity and privacy management infrastructures - "*Protocols for privacy infrastructures enabling multi-identity and tools to check privacy assurance and enable un-observability and un-*

linkability through search engines or social networks. Advancement of privacy at the hardware level" was not addressed. Moreover, the privacy aspects in Call 8 are addressed by very few projects (like FUTUREID and MUSES); yet the goals of these projects are not fully compatible with this sub-objective.

- For several sub-objectives it is yet unclear whether those will be covered or not, because the respective projects descriptions are vague. For example, for the sub-objective ICT-2011.1.4: Trust, e-identity and privacy management infrastructures – "*development of trust architectures, […] to delegate trust and partial trust, and for high-level tools at the end-user stage (cognitive and learning instrumentation for trust, profiling services and communities)"* we can see that the OPTET project with mechanisms of proving trustworthiness could also deliver such techniques, but it is not clear from the project description whether it indeed plans to do so.

Table 6. Objectives of Call 1 and projects that address those

Objective	Description from respective Work Programme	Projects that address the Objective
ICT-2007.1.4: Security and resilience in network infrastructures	Building and preserving flexible, scalable and context-aware, secure and resilient architectures and technologies to enable dynamic management policies that ensure end-to-end secure transmission of data and services across heterogeneous infrastructures and networks, including dynamic networks of tiny insecure devices and multiple provider, business and residential domains; real time detection and recovery capabilities against intrusions, malfunctions and failures	**AWISSNET**: a toolbox to configure and support ad-hoc personal area networks and wireless sensor networks **GEMOM**: a self-organizing messaging platform that is resilient to faults **INTERSECTION**: an integrated security framework for security and resiliency of heterogeneous networks **PRISM**: a privacy-preserving network monitoring system **TECOM**: a systematic approach for development of trusted embedded systems including trust components in hardware, trusted operating systems based on secure virtualization, and trusted protocols **WOMBAT**: collection, characterization and analysis of cyberthreats (e.g. malware)
ICT-2007.1.4: Security and trust in dynamic and reconfigurable service architectures	Service architectures supporting assured and scale-free composition of services and service coalitions with managed operation across several administrative or business domains, enabling flexible business models	**AVANTSSAR**: technology for formal specification and automated validation of service platforms. **MASTER**: a system for ensuring compliance with regulations, policies and obligations by an organization **SECURESCM**: protocols and tools for secure computation on shared data in collaborative supply chain management **TAS3**: a trusted service architecture to manage and process distributed personal information
ICT-2007.1.4: Trusted computing infrastructures	Computing infrastructures ensuring interoperability and end-to-end security of data and services; increased security and dependability in the engineering of software and service systems to	**CONSEQUENCE**: a data-centric information protection framework based on data sharing agreements. **CACE**: a toolbox for development of high-level cryptographic applications by means of cryptography-aware high-level programming languages and compilers

Objective	Description from respective Work Programme	Projects that address the Objective
	ensure the design and development of trustworthy applications and services	**SHIELDS**: a security vulnerabilities repository service for dissemination of software vulnerability information, and a software certification method to fight against common security vulnerabilities
ICT-2007.1.4: Identity management and privacy enhancing tools	Tools with configurable, context-dependent and user-controlled attributes in static and dynamically changing environments; trust policies for managing and assessing the risks associated to identity and private data	**PICOS**: a privacy-respecting identity management platform that supports provision of online community services **ACTIBIO**: unobtrusive authentication techniques relying on enhanced biometrics **MOBIO**: biometric authentication systems for services on mobile devices **PRIMELIFE**: privacy-enhancing techniques for virtual communities (social networks) and collaborative applications on the Internet **SWIFT**: a cross-layer user-centric identity framework for multitude of networks and services, supporting multiple personae **TURBINE**: revocable pseudo-identities from biometric data
ICT-2007.1.4: Longer term visions and research roadmaps	Metrics and benchmarks for comparative evaluation and open technology competitions, in support of certification and standardization; international cooperation and coordination with developed countries; coordination with related national or regional programmes or initiatives and coordination of FP7 projects addressing security, dependability, privacy and related ethical issues across different challenges and objectives of this Work Programme.	**AMBER**: a set of standards, best practices and benchmarks for assessment of software systems resiliency **ECRYPTII**: Network of Excellence in Cryptography to ensure integration of the EU research in this area into academia and industry, develop a common tools and benchmarks, and foster the EU cryptography community **FORWARD**: coordination of working groups of experts in cyberthreats, implementation of a cross-EU platform for monitoring of threat landscape evolution, and identification of cyber-attacks scenarios **INCO-TRUST**: coordination of research agendas and fostering collaboration in the area of trustworthy, secure and dependable ICT **THINKTRUST**: collection and analysis of technical and non-technical requirements of end-consumers in the area of trustworthy, secure and dependable ICT
ICT-SEC-2007.1.7-Focus ICT: Technology building blocks for creating, monitoring and managing critical information infrastructures, including	Understanding and managing the interactions and complexity of interdependent critical infrastructures; mastering their vulnerabilities; preventing against cascading effects; providing recovery and continuity in critical scenarios (including research towards designing and building self-adapted and self-	**MICIE**: an alerting system to identify in real time the level of possible threats induced on a particular critical infrastructure and notify the authorities providing them a real risk level **UAN**: an underwater acoustic network in order to gather environmental information for surveillance, monitoring and deterrence. **VIKING**: a framework for identification and assessment of vulnerabilities in SCADA systems and estimation of societal consequences from power breakdowns

Objective	Description from respective Work Programme	Projects that address the Objective
longer term visions and research roadmaps	healing complex systems); security and dependability metrics and assurance methods for quantifying infrastructure interdependencies	**COMIFIN**: a middleware for monitoring, notification and mitigation for financial infrastructure protection **INSPIRE**: identification of vulnerabilities and development of techniques for securing networked process control systems **PARSIFAL**: coordination of research activities in critical finance infrastructure protection and development of research roadmaps in this area **PEACE**: a general emergency management framework for extreme emergency situations, with a focus on establishing secure and reliable multimedia communication in such situations **SERSCIS**: adaptive service-oriented technologies for creating, monitoring and managing critical information systems for enhancing their resiliency and availability **WSAN4CIP**: security-by-design for wireless sensor networks deployed in power generation and distribution infrastructure management systems
	Designing and developing secure and resilient networked and distributed information and process control systems; systematic risk analysis and security configuration and management of critical information infrastructures and dynamic assurance frameworks for interconnecting them with critical infrastructures; availability of security forensics.	
	Developing longer term visions and research roadmaps; metrics and benchmarks for comparative evaluation in support of certification and standardization; international cooperation and coordination with developed countries; coordination with related national or regional programmes or initiatives.	

Table 7. Objectives of Call 5 and projects that address those

Objective	Description from respective Work Programme	Projects that address the Objective
ICT-2009.1.4: Trustworthy network infrastructures	Trustworthy network infrastructures as well as communication, computing and storage infrastructures in the context of the development towards the Future Internet as a conglomerate of heterogeneous networks and systems. Work includes development of novel architectures with built-in security, dependability and privacy; and trustworthy management of billions of networked devices, 'things' and virtual entities connected in the Future Internet.	**TAMPRES**: security mechanisms for microcontrollers hardware that will be used in the Internet of Things devices **DEMONS**: a privacy-preserving cross-domain network monitoring and management infrastructure **PASSIVE**: an approach to securing virtualized systems encompassing policy-based security provisions and fully virtualized yet controlled resource access in large-scale deployments **TCLOUDS**: a resilient cross-border privacy-enhanced trustworthy

Objective	Description from respective Work Programme	Projects that address the Objective
	Trustworthy platforms and frameworks for autonomously monitoring and managing threats, which need to be typically cross-border, cross-organizational, scalable, distributed, dynamically evolving and collaborative. Whilst developing technologies, projects should give adequate attention to aspects of usability, societal acceptance and economic and legal viability, through appropriate research, experimentation or demonstration in realistic, complex and scalable scenarios and contexts	infrastructure cloud platform **TWISNET**: a platform for command and control over wireless sensor networks enhanced with privacy, confidentiality and reliability guarantees **VIS-SENSE**: a visual analytics technology for identification and predictions of abnormal behaviour patterns in networked infrastructures
ICT-2009.1.4: Trustworthy service infrastructures	Trustworthy and privacy protecting service systems, platforms and infrastructures as part of the development towards the Future Internet, which support adaptability, interoperability, scalability and dynamic composition of services for citizens and businesses. Work includes flexible and dynamic mechanisms and risk-based methodologies to respond to threats and vulnerabilities, as well as to changes and conflicting demands in operating conditions, business processes or use practices through the full lifecycle.	**ABC4TRUST**: a privacy enhancing authentication technology allowing to reveal only partial information about the client identity (attribute-based credentials) **ANIKETOS**: a platform and accompanying tools to support service designers in building secure and trustworthy composite services and system administrators in monitoring execution of composite services and react in case of violations **ASSERT4SOA**: security certification standards for services tackling assurance for composite services **MASSIF**: a SIEM framework for scalable multi-level event processing and predictive security monitoring **SPACIOUS**: an approach for automated security validation of composite services at service provision and consumption time **WEBSAND**: a framework for controlling information exchange in composite Web services
	Interoperable frameworks for identity management for persons, tangible objects and virtual entities, with emphasis on user centricity and respect of privacy for personal users.	
	Whilst developing technology, projects should give adequate attention to aspects of usability, societal acceptance, human behaviour and principles of human rights and legal and economic viability. This could involve multi-disciplinary research activities, experiments or demonstration in realistic, complex and scalable scenarios and contexts	
ICT-2009.1.4: Technology and tools for trustworthy ICT	In highly distributed networked process control systems and in networks of very high number of things. Understanding threat patterns for proactive protection.	**POSECCO**: A framework for enabling traceable and sustainable traceability link between requirements and configuration settings in a system **UTRUSTIT**: a toolkit to monitor and regulate how the Internet of Things devices transmit private information
	For user-centric and privacy preserving identity management, including for management of risks and policy	

Objective	Description from respective Work Programme	Projects that address the Objective
	compliance verification	**GINI-SA**: a user-centric personalised identity management ecosystem where user identities are linked to verifiable national data registries and a marketplace for services designed for handling and storage of identity data **PINCETTE**: a technology to ensure safe distributed infrastructure upgrades by validating continuously evolving networked software systems **SECFUTUR**: a security engineering process for embedded system including resource-efficient security building blocks and a framework for using those in the embedded system design **SEPIA**: a security architecture for mobile and embedded systems based on process isolation and protection of sensitive data **TABULA RASA**: a spectrum of attacks on trusted biometric systems, countermeasures against those via a combination of multiple biometric traits or a novel robust biometrics
	For management and assurance of security, integrity and availability, also at very long term, of data and knowledge in business processes and services.	
	For assurance and assessment of the trustworthiness of complex and continuously evolving software systems and services	
	In enabling technologies for trustworthy ICT. This includes cryptography, biometrics; trustworthy communication; virtualization; and certification methodologies.	
ICT-2009.1.4: Networking, coordination and support	Support to networking, road-mapping, coordination and awareness raising of research and its results in trustworthy ICT. Priority will be given to:	**SYSSEC**: Network of Excellence that promotes cybersecurity education, creates a research roadmap, identifies threats and vulnerabilities of the Future Internet, and supports collaborations among EU research organizations **ACTOR**: support of the Trust in Digital Life partnership in development of Strategic Research Agenda **BIC**: coordination of EU research in trustworthy ICT and alignment of the EU vision with research programmes in Brazil, India and South Africa **EFFECTS+**: coordination and clustering of the Trust & Security Programme R&D projects and development of future research directions for the trust, security, privacy and compliance of the EU Information Society and Future Internet **NESSOS**: Network of Excellence to coordinate and foster research activities for secure Future Internet software services and systems
	Emerging threats and vulnerabilities in the Future Internet	
	Security and resilience in design, performance and scalability of future software-based service systems	
	Economics of security addressing cost effectiveness and market compliance of security solutions	
	Promoting wide use of standards, certification models and best practices	
	Legal and societal aspects related to technology development of trustworthy ICT	
	Coordination of national research actions in the field	
	International cooperation in fields where global action will create added value	

Objective	Description from respective Work Programme	Projects that address the Objective
		engineering and promote education activities in this domain
FI.ICT-2011.1.8 Use Case Scenarios and early trials	[Phase 1] A comprehensive set of detailed technical, functional and non-functional specification for an experimentation in the given use case, including the characterization of use case scenarios; the identification of Generic Enablers and architectural requirements to be developed through the Core Platform Objective, complemented by domain-specific capabilities […]; the assessment of existing R&D activities to build on; and the drafting of a strategy towards contributing to standardization in the respective application fields	**ENVIROFI**: consolidation of the Future Internet requirements from the environmental usage area perspective and provision of technical specifications and prototypes of interoperable geospatial environmental enablers, for terrestrial, atmospheric and marine environments **INSTANT MOBILITY**: identification of requirements and development of enablers for a virtual Future Internet platform for transport and mobility information and services **SAFECITY**: a collection of requirements and identification of enablers for smart public safety and security for smart Future Internet cities
	[Phase 1] Development of domain-specific capabilities and conceptual prototypes demonstrating critical technological solutions and the overall feasibility of the approach suggested for phase 2	
	[Phase 1] A phase 2 implementation plan, including a detailed analysis of the potential experimentation infrastructures, and a plan for user community building	
	[Phase 2] Working experimentation sites building upon common components and Generic Enablers as provided under the Core Platform Objective complemented by the identified use case specific capabilities	
	[Phase 2] Selected test applications implemented on these experimentation sites	
	[Phase 2] Validation of the openness and versatility of the Core Platform and its software development kit, through implementation of mixed use case scenarios originating from more than one use case project	
	[Phase 2] A detailed plan for how to move into phase 3, including detailed plans for large scale expansion of platform usage facilitated by local and regional stakeholders including SMEs	
	The proposed work needs to demonstrate: the valorizations of earlier	

Objective	Description from respective Work Programme	Projects that address the Objective
	Future Internet research within a complete system perspective; the commitment, backed by appropriate mechanisms, to collaborate with other FI-PPP activities; openness and related approach towards standardization; the potential for innovation and related market impact, which is the main driving requirement of the FI-PP implementation	

Table 8. Objectives of Call 8 and projects that address those

Objective	Description from Work Programme	Projects that address the Objective
ICT-2011.1.4: Heterogeneous networked, service and computing environments	Trustworthy (meta) architectures and protocols for scalability and interoperability, taking account of heterogeneity of domains, partitions, compartments, capabilities, and environments in ecosystems and underlying infrastructures; architectural standards, including meta-level specifications, for conformity, emergency and security policy management.	**EURO-MILS**: standards for security evaluation of highly critical embedded systems based on the MILS approach (in essence, virtualization of complex systems into independent components) **HINT**: a framework for embedded systems integrity checking **MUSES**: a system to enforce corporate security policies while taking into account end-user privacy, usability, information delocalization and the BYOD paradigm. **NEMESYS**: a framework for detection and analysis of threats in mobile devices and networks **RASEN**: enablers of entanglement of risk assessment and security testing to ensure organizational security **TRESCCA**: an approach to enable trust in cloud computing on sensitive data via securing embedded systems and migrating virtual machines **TRESPASS**: a tool to automate risk assessment for organizational socio-technical systems **ACDC**: an EU cyber-defense center for analysis of botnets and identification of countermeasures against them **CUMULUS**: an integrated framework of models, processes and tools supporting security certification of infrastructure, platform and application services in the cloud (the "as a service" model) **D-MILS**: a common framework for distributed critical systems
	A trustworthy polymorphic Future Internet with strong physical security in balance with privacy; federated seamless, transparent and user-friendly security of the edge networks in smart eco-systems, ensuring interoperability throughout the heterogeneous landscape of access networks	
	Virtualization and other techniques to provide protection, assurance and integrity in complex, high-demand critical services; and security in the presence of scarce resources, and in legal domains with different priorities. Trustworthy global computing with contextual security and secure smart services of large scale systems	
	Metrics and tools for quantitative security assessment and predictive security in complex environments and for composition and evaluation of large scale systems	
	Enabling technologies, such as declarative languages, biometry, technology for certification and	

Objective	Description from Work Programme	Projects that address the Objective
	accreditation or cryptography for Trustworthy ICT.	construction and certification based on the MILS technology
ICT-2011.1.4: Trust, e-identity and privacy management infrastructures	Development of trust architectures, protocols and models for trust assurance, including measures and rating models, and services, and devices, to enable trust assessment (e.g. by claims on identity, reputation, recommendation, frequentation, voting) to delegate trust and partial trust; and for trust instrumentation and high-level tools at the end-user stage (cognitive and learning instrumentation for trust, profiling services and communities)	**FUTUREID**: A flexible, privacy-friendly and usable identity management infrastructure for Europe **OPTET**: an approach for enabling provable trustworthiness in socio-technical systems connected to Internet
	Protocols for privacy infrastructures enabling multi-identity and tools to check privacy assurance and enable un-observability and un-linkability through search engines or social networks. Advancement of privacy at the hardware level.	
	Interoperable or federated management of identity claims integrating flexible user-centric privacy, accountability, non-repudiation, traceability as well as the right to oblivion at the design level. Technologies and standardization for use of multiple authentication devices, applicable to a diversity of services and ecosystems, and providing auditing, reporting and access control.	
ICT-2011.1.4: Data policy, governance and socio-economic ecosystems	Management and governance frameworks for consistent expression and interpretation of security and trust policies in data governance and means for implementation, including in the ubiquitous scale-less Web or Cloud. Technology supported socio-economics frameworks for risk-analysis, liability assignment, insurance and certification to improve security and trust economics in the EU single market	**A4CLOUD**: a framework for enabling accountability in the cloud supported by accompanying tools and best practices **ATTPS**: trust paradigm shift enablers **INTER-TRUST**: a framework for negotiation of trust and security policy among composite services, including dynamic introduction of new security features into existing policies
	Multi-polar governance and security policies between a large number of participating and competitive stakeholders, including mutual recognition security frameworks for competing operators; transparent security for re-balancing the un-fair,	

Objective	Description from Work Programme	Projects that address the Objective
	unequal face-to-face relationship of the end-user in front of the network; tools for trust measurement, based on cost-benefit analysis	
ICT-2011.1.4: Networking and coordination activities	Support for networking, road-mapping, coordination and awareness raising of research and its results in Trustworthy ICT. Priority will be given to:	**CIRRUS**: a consortium with various stakeholders (industry, cloud consumers, policy makers, etc.) for developing standardization, certification and best practices for security of cloud infrastructures **CYSPA**: an association for analysis and prevention of cyber disruptions and development of an integrated EU strategy for protection of the cyberspace **FIRE**: coordination of the EU Trustworthy ICT research, understanding the exploitation requirements in this sector and export opportunities, and development of research roadmaps in the key sub-sectors **SECCORD**: coordination and clustering of the EU Trust & Security Programme R&D projects, enhancing their visibility, assessing their impact and providing an outlook of the emerging T&S issues **STREWS**: a technical state of practice document for Web security and a roadmap for future research and standardization in this domain
	Stimulating and organizing the interplay between technology development and legal, social and economic research through multi-disciplinary research communities	
	Promoting standards, certification and best practices	
	Coordination of national RTD activities	

Domains for Application of the Delivered Innovations

The Network and Information Security field produces results that are useful in a multitude of industry sectors. Table 9 overviews the domains where the innovative results produced by the R&D projects in Trust and Security have been already applied based on the validation activities executed by the projects.

Notice that the classification in this section differs from the classification of the Call 8 projects by beneficiaries of the projects' results in Section 0, where we have analyzed the immediate buyers of the projects' contributions. Instead in this section we illustrate the domains for application of security products based on the case studies chosen by projects to validate their artifacts. For example, the RASEN project produces methodologies and tools for enhanced risk assessment and security testing, and the immediate buyers of these techniques are companies from the ICT Security Industry. However, RASEN plans to validate its artifacts in the healthcare, financial and software products sectors; and these are the domains reflected in Table 9.

From this table we can see that the **Trust & Security Programme projects collaborate with a variety of different industry sectors where ICT security technology is needed**. The most "popular" domains with the largest shares of projects are: Critical Infrastructures, Emergency Handling and Disaster Recovery; Energy & Utility Services and Smart Grid;

Internet Services; Public Administration; Software Products and ICT Services. Also Transport and Telecom and Internet Service Provision sectors received attention from the projects. Players from these domains look out for security innovations because their products and services have a lot of requirements on security, trustworthiness and dependability; and also provable security of a product can become a significant business advantage.
The domain (synthetically) aggregating the biggest number of projects is the Research, Education and Public Knowledge sector. The contributors to this domain are projects that have delivered results to use for research teams (like the CONSEQUENCE project data sharing facility), to enhance education curriculums (all Networks of Excellence) and results improving public knowledge (e.g. databases of vulnerabilities and research roadmaps) that were validated in the respective communities (i.e. by researchers, by education professionals and by experts in the related field).
We expect that Table 9 will also be used by new projects preparing the use case requirements and validation scenarios as a pointer to discover previous contributions to the same activity.

Table 9. Domains for applications of delivered solutions based on the executed validation activities

Domain	Call 1 Projects	Call 5 Projects	Call 8 Projects	Total number of projects
Ambient Assisted Living and *Smart Homes*	AWISSNET	UTRUSTIT, SECFUTUR	TRESCCA, TRESPASS, OPTET	6
Critical Infrastructures, Emergency Handling and *Disaster Recovery*	CONSEQUENCE, MICIE, VIKING, AWISSNET, COMIFIN, GEMOM, INSPIRE, PARSIFAL, PEACE	MASSIF, SECFUTUR	OPTET	12
Energy & Utility Services and *Smart Grid*	MICIE, VIKING, WSAN4CIP	PINCETTE, SECFUTUR, TCLOUDS, TWISNET	TRESCCA, CYSPA, D-MILS	10
Entertainment	PICOS			1
Environment Monitoring and Care	UAN, GEMOM	ENVIROFI		3
Financial Services	COMIFIN, PARSIFAL		RASEN, CYSPA	4
Healthcare and *e-health*	AVANTSSAR	TCLOUDS	FUTUREID, RASEN, CUMULUS	5
Internet Services (e-commerce platforms, cloud computing, social networks)	AVANTSSAR, PICOS, PRIMELIFE, WOMBAT	ABC4TRUST, ACTOR, SPACIOUS, TCLOUDS	A4CLOUD, ATTPS, TRESPASS, CIRRUS	12
Manufacturing Industry	MOBIO	TAMPRES, PINCETTE, SEPIA	EURO-MILS, HINT	6
Military and *Physical Infrastructure Security*	ACTIBIO, TURBINE		D-MILS	3
Other (Research, Education and *Public Knowledge)*	CONSEQUENCE, CACE, ECRYPTII, FORWARD, INCO-	SYSSEC, BIC, EFFECTS+, NESSOS,	ACDC, CIRRUS, FIRE, SECCORD, STREWS	18

Domain	Call 1 Projects	Call 5 Projects	Call 8 Projects	Total number of projects
	TRUST, SHIELDS, THINKTRUST, WOMBAT	WEBSAND		
Public Administration (e-voting, e-government, public authorities)	AVANTSSAR, SWIFT	ABC4TRUST, ANIKETOS, UTRUSTIT, GINI-SA, PASSIVE	FUTUREID, INTER-TRUST, CYSPA	10
Smart Cities		SAFECITY	CUMULUS	2
Software Products and *ICT Services*	CACE, ECRYPTII, SHIELDS	ASSERT4SOA, MASSIF, POSECCO, SYSSEC, ENDORSE, VIS-SENSE	FUTUREID, MUSES, RASEN, STANCE	13
Telecom and *Internet Service Provision*	PRISM, SWIFT	ANIKETOS, DEMONS, VIS-SENSE	NEMESYS, TRESPASS, ACDC, CYSPA	9
Transport (aero, land, water)	ACTIBIO, AWISSNET, SERSCIS, SECURESCM, TURBINE	ANIKETOS, INSTANT MOBILITY	EURO-MILS, INTER-TRUST	9
Various Private Services (insurance, consulting)		ENDORSE		1

Addressing the Emerging Challenges of the NIS Platform

The EU R&D projects have acquired significant expertise in addressing the emerging network and information security issues and have significantly advanced the state of the art in this domain. Moreover, **the EU policy makers and coordination bodies (such as the Network and Information Security Public-Private Platform, NIS PPP) can use these results and expertise to gain the insights on the technological as well as social, economical and legal challenges in the strategic EU activities.** In this section we list the projects whose experience and innovative contributions are the most relevant to the new security and trust challenges ahead of the NIS Platform (in Table 10).

The NIS Platform comprises three Working Groups[3]:

- *WG1 Risk Management*: will identify best practices to design, implement and maintain cybersecurity risk management processes throughout an organization. In particular WG1 addresses: *information assurance*; *risk metrics to monitor predict, track and evaluate risk exposure*; and *awareness raising practices* to acquire and disseminate cybersecurity knowledge and skills.
- *WG2 Information Exchange*: will identify best practices to exchange information on cybersecurity incidents of different nature (technology failures, human mistakes, natural events, malicious attacks) and on threats and vulnerabilities. The information exchange shall include steps to *communicate information within and outside an organization* including to businesses, government and technical bodies as well as to the public. In particular WG2 will identify *best practices for incident reporting*, including reporting tools and templates; *incident coordination*, including processes for exchanging information on actual incident to engage in a collaborative actions to

[3] https://resilience.enisa.europa.eu/nis-platform

handle incidents; and *exchange of information on threats and vulnerabilities* affecting systems. WG2 will also address *metrics, measurements and language for information exchange*.

- WG3 Secure ICT Research and Innovation: will identify *key challenges and corresponding desired outcomes in terms of innovation-focused, applied but also basic research in cybersecurity, privacy and trust*; and propose *new ways to promote truly multidisciplinary research that foster collaboration* among researchers, industry and policy makers. WG3 will serve as a facilitator for the *coordination of and collaboration between research agendas across Europe,* including industry research roadmaps and national research programmes. WG3 will also identify the *elements of a possible European industrial strategy for cybersecurity* and *examine ways to increase the impact and commercial uptake of research results in the area of secure ICT*.

The projects from Call 1 and Call 5 are (almost) over; therefore their contribution can consist of already delivered artifacts and expertise gained by the project members. The projects of Call 8 besides providing the artifacts and expertise can also become platforms to execute the relevant actions proposed by the NIS Platform and evangelize recommended practices. For example, SECCORD designed to coordinate and cluster the Trust & Security projects fits naturally in the WG3: Secure ICT Research and Innovation of the NIS Platform, as suggested also by the SECCORD Advisory Board [3].
We can see in Table 10 that WG3 can enjoy contributions from the largest share of project. Also WG1 can receive a rich input from the EU Trust & Security projects. Instead the WG2: Information exchange has less projects that have contributed to its goals, most of them from Call 1.
Notice that Table 10 lists only the projects that either directly focus on the targets set upon the NIS Platform Working Groups, or provide enablers for these targets. Yet, all the FP7 Trust & Security Programme projects have delivered/are set to deliver results that can be potentially useful for achievement of the NIS Platform goals

Table 10. Projects that can contribute to the NIS PPP Working Groups

NIS PPP Working Group	Projects from Call 1	Projects from Call 5	Projects from Call 8
WG1 Risk Management	**INSPIRE**: identification of vulnerabilities and development of techniques for security networked process control systems **MASTER**: a system for ensuring compliance with regulations and policies by an organization **MICIE**: an alerting system to identify in real time and predict the level of threats induced on a critical infrastructure **VIKING**: estimation of security risks and evaluation of disruption consequences in SCADA networks	**MASSIF**: a SIEM framework for scalable multi-level event processing and predictive security monitoring **NESSOS**: delivers new curriculum for secure Future Internet services and software engineering **POSECCO**: a framework for enabling traceability between requirements and system configuration **SYSSEC**: delivers a new cybersecurity curriculum and promotes cybersecurity education **VIS-SENSE**: a visual analytics technology for identification and prediction of abnormal behavior	**CYSPA**: a methodology to evaluate an impact of cyber-disruptions on an organization **MUSES**: a system to enforce corporate security policies and identify risky employee behavior via applying risk metrics **OPTET**: an approach to enable provable trustworthiness in socio-technical systems **RASEN**: enhancements to organizational risk assessment, including legal risk assessment **TRESPASS**: a tool to automate risk assessment for organizational socio-

NIS PPP Working Group	Projects from Call 1	Projects from Call 5	Projects from Call 8
		patterns in network infrastructure	technical systems
WG 2 Information Exchange	**CONSEQUENCE**: a scalable, secure and resilient infrastructure for data sharing across multiple organizations **FORWARD**: a cross-EU platform for monitoring of threat landscape evolution **MICIE**: an alerting system to identify in real time the level of possible threats induced on a critical infrastructure and notify the authorities **PEACE**: an emergency management framework for establishing a secure and reliable communication in critical situations **SECURESCM**: protocols and tools to secure computation on shared data **TAS3**: a trusted service architecture to manage and process distributed sensitive information **SHIELDS**: a software security vulnerabilities repository **WOMBAT**: a repository of cyberthreats and methodologies for threat detection and analysis	**SYSSEC**: works on identification of the Future Internet vulnerabilities	**ACDC**: a EU cyber-defence centre for analysis of analysis of botnets and identification of countermeasures against them
WG3 Secure ICT Research and Innovation	**FORWARD**: coordination of working groups of experts in cyberthreats **INCO-TRUST**: coordination of research agendas, and fostering collaboration in the area of trustworthy, secure and dependable ICT **PARSIFAL**: coordination of research activities in critical finance infrastructure protection **THINKTRUST**: collection and analysis of technical and non-technical requirements of end-consumers in the area of secure, trustworthy and dependable ICT	**ACTOR**: supports the Trust in Digital Life consortium in support of the Strategic Research Agenda for Europe **BIC**: coordination of the EU research in trustworthy ICT and alignment of the EU vision with research programmes in Brazil, India and South Africa **EFFECTS+:** coordination and clustering of the FP7 Trust & Security R&D projects and development of future research directions **NESSOS**: a Network of Excellence in the services and systems security engineering that coordinates activities in this	**CIRRUS**: a consortium encompassing different stakeholders for best practices in cloud security **CYSPA**: an association for analysis and prevention of cyber-disruptions and development of an integrated EU strategy for protection of cyberspace. **FIRE**: coordination of the EU Trustworthy ICT research, understanding avenues for its exploitation and development of roadmaps in key sub-areas **SECCORD**: coordination and clustering of the EU Trust & Security projects, and providing an outlook

NIS PPP Working Group	Projects from Call 1	Projects from Call 5	Projects from Call 8
		area **SYSSEC**: a Network of Excellence in the Systems Security domain that creates a research roadmap in this area	on the emerging T&S issues **STREWS**: a roadmap for future research and standardization for Web security

The ICT Security Domain in EU

In this section we report the results of the interviews of project leaders of the Call 5 and Call 8 projects. We have asked the project leaders to identify the market acceptance gaps for their technology and in general, and also which strengths and weaknesses of the EU ICT security market do they see. In this section we report the notable findings regarding weak spots of the EU ICT security landscape, specifically weaknesses of the EU projects, and how these can be overcome.

EU R&D Projects' Weaknesses

The projects often **do not execute market studies for their technologies and do not take costs into account** to ensure acceptance of their technology. The business model says security must also be economically viable, or at least have chances to become economically viable.

Often there is **a gap between research results and industry acceptance** and the problem of maturity of technology. Many outstanding research results have not been brought to industry, sometimes due to the usability issues. This could be to be taken into account by **putting more effort and rigour into the validation activities** executed in the projects. This will consume efforts from research, but may prove better for industry acceptance.

However, it may be **difficult for projects to plan validation and exploitation activities well ahead** of actually solving the research problems; moreover because writing a successful proposal requires to promise a lot of exploitation activities that might turn not to be viable in the end. This may be addressed by **introducing two project types**: one for basic research with a focus on innovation and problem solving, another with shorter time line and smaller group of partners to execute validation and exploitation of already produced results (e.g. through pilots and user trials). Similar findings were reported in the EFFECTS+ deliverable D2.2 [2].

Several project leaders have noted that the EU technology often appears when it is too late and the market is already taken by some other non-EU solutions. They have proposed to tackle this by **fostering disruptive innovation**. As an instrument, some projects can be launched that would focus not on improving existing technologies and tools, but on something completely new.

Another aspect mentioned concerns industrial participants of the projects. Typically research units of a company face the challenge that their product units typically are interested in shorter time horizons (1-2 years) than research units can offer (3 years from the project start plus some time for technology maturity). An option here is to **encourage industry partners to develop and demonstrate project results** in their products (e.g. by dedicated exploitation projects discussed above).

Often after the end of the project the technology is not maintained (people involved have changed the job, no funding available, etc.). Some of the interviewees have suggested **a dedicated demonstration platform under the umbrella of the European Commission to provide support for technology** after the project lifetime.

As we have discovered, for the projects in Call 1 some websites are already not maintained and it may become difficult to discover the project contributions. An option to solve this problem might be **a centralized repository for public deliverables** (e.g. the Open Access framework or the SECCORD website). Notice that some active projects even do not publish on their websites all public deliverables. We suggest that it becomes obligatory to publish all public deliverables and maintain them accessible even after the project is finished.

Structural Issues with ICT Security in EU

Several project leaders have mentioned that the ICT Security Domain in Europe is too technology-oriented; it does not look enough at non-technological factors like usability. We

can notice that this issue was mentioned to be very relevant also to the EU Trust & Security projects; and it was addressed with the projects selected in Call 8; however further steps in these directions are needed.

Another gap that the EU security industry might face is the **skills gap**. Most of the interviewees acknowledged the professionalism of EU security experts and leading positions the EU security industry has in most of the security fields, e.g. embedded systems, secure protocols, software verification. However, several project leaders have noted that the amount of students studying security is insufficient, especially in comparison with such countries as US or China. Also, Europe experiences a brain-drain: a lot of security practitioners leave Europe for other countries. **Promotion of graduate and post-graduate security education in Europe** can be an option to mitigate this gap.

Interoperability of legal and technological frameworks across the EU was mentioned to be missing due to the variety of regulations and practices across countries. This in turn implies hindrances of security solutions implementation, and therefore deployed solutions are often insecure or are not compliant with regulations. **Harmonization and standardization actions across the EU are required.**

EU Societal Security Challenges

Advent of Internet of Things and critical infrastructures connectivity to Internet will bring **new cyber threats**. The European Commission is already taking actions (since Call 1 and the Joint ICT-SEC Call). However, it was reported that the manufacturers were not yet taking this into account.

Strengths of the EU technical results, as identified by many interviewees, are strong orientation to an individual and protection of individual's privacy. As one of the project coordinators has put it: "*Europe has strong value system around trust and security".* However, these **privacy concerns are often missing in the business design**. The coordinators expect that If the **EU will have very well defined security requirements and regulations, everybody will have to adapt**, including big non-European industry players, and this can be an opportunity for Europe.

Finally, one of the most raised concerns is the **low security awareness and lack of security education – in citizens as well as in organizations**. This challenge also aligns with the previously mentioned skills gap, however it is impacting not only the EU ICT security industry, but also the EU society as a whole. The lack of awareness is also a business problem: people are less willing to pay for security and privacy. However, in the end they pay even more in damages or taxes. Latest media scandals (e.g. the recent PRISM and Tempora revelations) and attacks on influential companies (Twitter or Apple) or critical infrastructures (the Stuxnet attack) slowly raise the awareness and situation tends to improve. However, the attacks are also becoming more serious. Therefore, it is necessary to **educate citizens and business professionals in security**, by raising the awareness, bringing more media attention to security issues and best practices in security, and introducing security courses into curriculums.

Auxiliary Discoveries from the Study

We would like to report some auxiliary findings of the study. Addressing these issues could facilitate longevity of the knowledge base available after the projects are finished.

Websites are not maintained well

As of August 2013, 9 projects from Call 1 do not maintain their websites operational (out of 33). A lot of projects from Call 1 and Call 5 do not publish public deliverables on their websites. This situation hinders adoption of the projects' results, leading to a situation when the few cases when a technology or lessons learned are passed from one project to another are the cases when the project partners are the same (a follow-up project or simply similar consortium constituency).

This problem can be overcome by imposing stricter requirements on the website maintenance and organizing a centralized repository for public deliverables where the projects could maintain their public outputs after project lifecycle is over.

The CORDIS Information is sometimes misleading

Sometimes the CORDIS system [2] is not correct in the details of the FP7 Trust & Security projects. For example, the ACTOR project homepage links to the ACTORS project, which is a completely different project. For the ACDC project there is no dedicated page on CORDIS at all.

As a side note, the project contact information (in the Participants and Coordinator parts) for most of the projects is administrative personnel. To facilitate communication with the projects for interested parties it could be useful to provide also the contact information of the project coordinators.

Concluding Remarks

In the Yearbook we have reported on the status of the EU Trust & Security Programme: what are the addressed topics, which projects were selected and how the Programme succeeds in achievement of the Work Programmes' goals. We have also zoomed in the innovative contributions of the projects that have agreed to be interviewed, presented the discoveries from interviews regarding the EU ICT Security Domain weaknesses, and analysed which projects could become contributors to the NIS Platform Working Groups.

Based on the executed study we can report that the Trust & Security Programme addresses the vast majority of the ambitious goals defined in the Work Programmes. A sub-objective that was not yet achieved, but is very important in the light of the new EU Cybersecurity Directive, is coordination of the national and regional research activities in Trust & Security in the Member States.

Trust & Security Programme is very agile and it is quick to address the new emerging issues and challenges, such as Cloud Computing or Mobile Device Security. A rich selection of industrial domains contributes to the EU projects and is able to immediately adopt their results. Very few issues of the Programme are reported in the Yearbook; the most important of those is the gap in the industrial adoption of the project results and inflexibility of the validation activities plans. We believe that the EC initiatives such as the NIS platform will help to overcome this gap.

References

[1] CORDIS FP7-ICT Projects in Trust and Security (Version from 12 June 2013). http://cordis.europa.eu/fp7/ict/security/projects_en.html. Accessed online in August 2013

[2] EFFECTS+ D2.2 – The Innovation Potential of FP7 Security & Trust Projects (revised version 3) May 2013

[3] SECCORD Advisory Focus Group Report (Version from 9 August 2013)