THE INNOVATION POTENTIAL OF FP7 ICT TRUST & SECURITY PROJECTS

EXECUTIVE SUMMARY AND POLICY PAPER

Fabio MASSACCI, Martina DE GRAMATICA, Olga GADYATSKAYA

May 2013

University of Trento is a public university registered in Italy and it does not express opinions of its own. The opinions expressed in this publication are the responsibility of the authors.

Department of Information Engineering and Computer Science
University of Trento
Via Sommarive 14, I-38123 Trento, Italy
tel: +39.0461.282086
fax: +39.0461.282093
https://securitylab.disi.unitn.it/

CONTENTS

ABOUT THE AUTHORS

Fabio Massacci is full professor at the University of Trento. He holds a Ph.D. in Computer Science and Engineering from the University of Rome "La Sapienza", and has been at Cambridge University, the University of Siena and IRIT Toulouse. For 7 years he was deputy rector for ICT procurements and services, what makes him one of the few researchers who were large buyers of ICT technology (and can see innovation from the customers' eye). He is one of the contributors of Trust and Security themes for the Italian National Research Plan for the next 5 five years. Currently he coordinates the SECONOMICS EU Project on security economics.

Martina De Gramatica is a research associate at the University of Trento. She has a degree in anthropology and social research from the Bicocca University in Milan. She has worked with a publishing house in the education and research sector and at the Science Museum in Trento on education, presentation and dissemination of scientific results to the general public.

Olga Gadyatskaya is a postdoctoral research fellow at the University of Trento. She received her Ph.D. in Mathematics at the Novosibirsk State University (Russia) in 2008. Before joining Trento in 2009 for the SecureChange Research project and the Security Coordination SecCord project, she worked as a researcher at Institute of Computational Mathematics in Novosibirsk (Russia).

ABOUT EFFECTS+

EFFECTS+ is an EU FP7 Networking, Coordination and Support project (reference nr. 258750) that was active in the period from 2010-09-01 to 2013-02-28.
The main objective of EFFECTS+ was enabling a coordination service for R&D for Trust, Security, Privacy and Compliance in the Information Society and the Future Internet.
The project consortium consisted of Waterford Institute of Technology (Ireland, the project coordinator), Hewlett-Packard Limited (UK), SAP AG (Germany), ATOS (Spain) and University of Trento (Italy).
Full details of this report are available in the Effects+ deliverable D2.2 "The innovation potential of FP7 ICT Trust & Security projects".

ACKNOWLEDGEMENTS

We would like to thank Unit F5, and the Project Officers who agreed to be interviewed, together with the project and technical coordinators of the FP7 Security and Trust projects for providing us the necessary bootstrapping information. Without their guidance and cooperation this report would not have been feasible.

We thank G. Comper and B. Crispo (University of Trento), K. Howker (TSSG), N. Papanikolau (HP Labs) for contributing to the analysis of the data.

At the University of Trento F. Dalpiaz, G. Oligeri and F. Paci contributed to the analysis of project deliverables. From the EFFECTS+ consortium the suggestions from M. Bezzi (SAP), F. Clearly (TSSG) and N. Wainright (HP Labs) were extremely helpful.

SUMMARY

The needs to meet compliance requirements, to minimize hackers damages and data breaches are compelling companies and governments to continue investing in security solutions. As a result, the **security market represents to this day a rapidly growing sector** almost unaffected by the recession. Recognizing this market potential the EU supports scientific organizations and private industries to carry out research activities under ICT Trust and Security Programme.

This report presents an executive summary of a **comprehensive study on the innovation potential of FP7 Security and Trust projects** funded by ICT Call 1 for Trustworthy ICT, Joint ICT and Security Call, and Call 5 for Secure, Dependable and Trusted Infrastructures.

A number of recommendations have emerged from the analysis and from the coordinators' and technical leaders' feedback that might boost the innovation potential of ICT Trust & Security projects. In particular, R&D projects should strengthen interactions with final users of their products and improve reporting of their validation activities. DG Connect should encourage participation of ICT security companies in the project consortia, promote project proposals on under-covered Digital Agenda actions (cyber-attacks preparedness and child protection), and endorse pre-commercial procurement of security solutions. The European Union as a whole could introduce new project funding scheme with a simplified procedure for experimenting research results in large-scale user trials, and propose a new legislation on mandatory security incidents disclosure.

Adoption of these measures might ensure that advances in ICT knowledge and know-how are rapidly transformed into products for the benefits for Europe's citizens, businesses, industry and governments.

KEY RECOMMENDATIONS

Improve the reporting of validation activities with users of research results. Projects should report in more effective and consistent way the methodology and actual dimension of pilots and trials with end users or product groups. Results of product group trials should be reported appropriately in the same way as user trials (if any). Obviously, some results of the pilots would not be public for IPR reasons, but lessons learned should be visible, as it happens in medical trials.

Enforce connection to final users (citizens, but also IT administrators or specialists) to ease marketing of security solutions. With the few exceptions of IT security services, in all other industries the transfer of research results to market requires mediation (security is a failure of a product). This gap might be addressed by actions that try to reach and experiment directly with final end-users.

Promote participation of ICT security companies. Participation of companies (or subsidiaries) that directly market security products or offer security consultancies should be promoted.

Promote pre-commercial procurement. The existing instrument of pre-commercial procurement should be used and further promoted to create long term pilots supported by public administrations.

Promote calls on preparedness against cyber-attacks and child protection. The project proposals on cyber-security and preparedness to counter cyber-crime and cyber- attacks and protection of children (e.g., specialized credentials or anonymity) on the Internet might be treated preferentially, as covering for the under-supported Actions. Initiatives such as Joint Calls might be an option to pursue in these sectors.

Introduce new funding scheme for experimenting in large scale trials. A specific instrument might be introduced that would still comply with pre-competitive requirements: a competitive call available to a subset of partners from concluded or near completion projects; with a narrow focus (a large-scale user trial of a result from a research project); simplified along the calls for international cooperation or enlargement to partners from new member states.

Consider an EU-wide regulatory initiative on mandatory incidents disclosure. A European-wide regulatory initiative is required to mandate the controlled disclosure of security incidents, along the lines of what is happens in the air traffic management.

I. THE LANDSCAPE OF PARTNERS, INDUSTRIES AND COLLABORATIONS

This study has been carried out by the University of Trento in cooperation with the EFFECTS+ partners by combining document analysis (projects' publishable summaries, deliverables and web sites) and an ethnographic study including personal focused interviews, based on a semi-structured questionnaire, at first with project officers (currently or previously in charge of the projects) and then with project coordinators or technical leaders. A parallel analysis has been conducted, based on the above material, on the Digital Agenda to further refine and specify the indications of the project coordinators on how their project contributed to the Digital Agenda. The projects considered in this study include more than 400 partners.

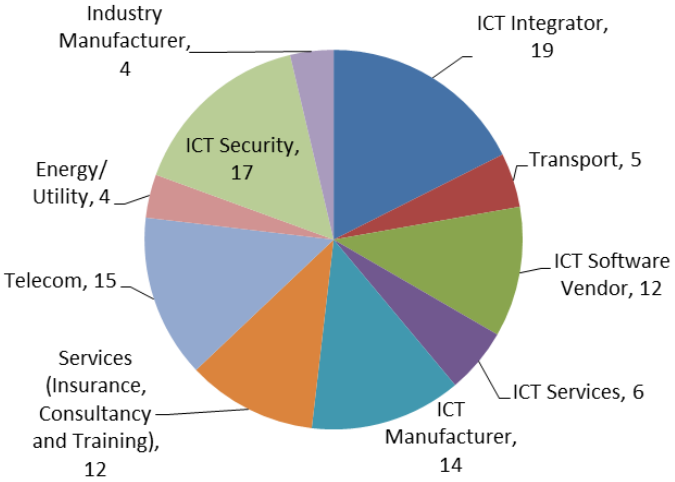

Figure 1. Global Call 1 breakdown per industry sector (108 industry partners in total)

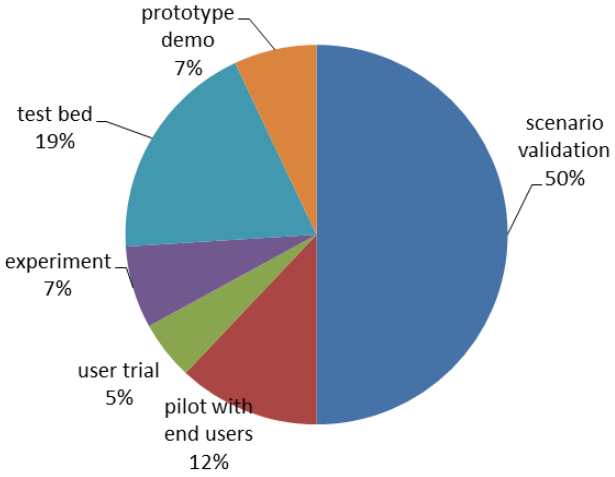

Figure 2. Validation activities breakdown for both Calls

Fact-finding summary

- In both Calls **academic partners (research centres and universities) and industry have almost equal share** (~50% of the funded project partners). Figure 1 presents the global industry sectors breakdown for Call 1 as an illustrative example.
- We have constructed graphs of the "social relationships" among the projects for both Calls. Figure 3 depicts this graph for Call 5. We did not find any isolated group of project participants. The **core of the community in both Calls is represented by few large software companies and IT integrators** (such as IBM, SAP and ATOS), which act as social hubs for the Calls project partners.
- The cross-call analysis shows that the field is very dynamic as the **priorities of the Call can significantly change the type of partners and their collaborative relations**. E.g., the ICT service providers play a significantly larger role in Call 5 (~12% of participants) than in Call 1 (~3%); in Call 5 the absolute number of telecom operators is lower, but they are more socially connected. This might be explained by the greater emphasis on critical infrastructures of Call 5 with respect to Call 1, which had a greater emphasis on privacy.
- Interestingly**, no hub is a specialized IT security company**, only SIRRIX and SEARCH-LAB are present in both Call 1 and Call 5. Specialized IT security companies form a fraction of the participants, but not the majority. In other words, IT security companies do participate to the calls, but they are not the hubs of the community. This phenomenon might be explained by the fragmented nature of the IT security market.

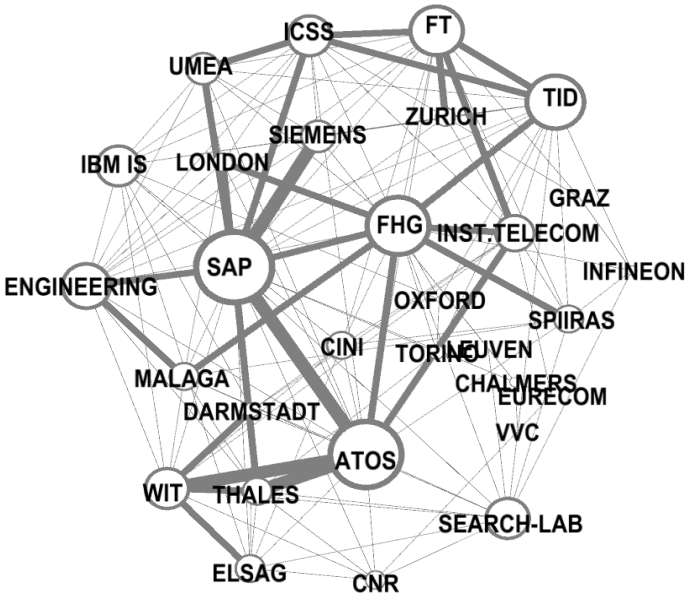

Figure 3. Social relationship graph in Call 5. We show only the partners who participated in two or more projects; the size of a node is determined by the number of links - i.e. the number of projects, not by the budget of the partner.

- Analyzing the data collected from the interviews with the project coordinators it is easily notable that **only a few projects considered validation of their results through a real pilot** (12%; Figure 2), namely asking to real people to make use for a certain period of time of the artifact, while most of the projects prefer to validate their results with a scenario validation (50%). This could surely depend on how many resources in terms of time and money are allocated to the validation phase, but also on what kind of validation is more suitable for each project (e.g.: if the final target beneficiaries are end-users, a pilot will be the more suitable validation test; on the contrary, to develop a monitoring framework, an experiment validation could be more effective).
- Yet, **the dominance of scenario validation impacts the methodological soundness of research validation:** the self-selection of the scenario will probably lead to a positive result, if the right scenario is chosen and this could affect the validity of the validation phase. Furthermore, if the validation phase is internal to the research team and will take place within the same framework, it is not likely to fail. If the results are tested by an external user the validation will be more realistic, since it might encounter problems not taken into account before. We return on the issue scenario vs. pilots in the last section on instruments.
- A side observation is that **the prima-facie documentary evidence from almost all projects (e.g. the publishable summary) is far from being satisfactory**. The documents are often difficult to get (because they are mingled with confidential information), and usually they do not address many questions on the validation of the project results[1]. Since the publishable report is the main road to the project results by third parties, this lack of information might stifle further innovation. In the absence of this information, the direct applicability of a research result to a specific industry must be understood as a target and as a proof-of-concept demonstration for which more evidence is needed.

[1] While a medical study might report that "The drug was distributed to 100 volunteers by 10 general practitioners and 5 specialists of internal medicine, and 80 patients survived", an ICT project would only report "The drug was distributed to some patients who survived."

Recommendation: *Projects should report in more effective and consistent way the methodology and actual dimension of pilots and trials with end users or product groups.*

Direct Beneficiaries of Project Results. Most projects include case studies that are used to validate their R&D results. From these activities we derive the immediate potential buyers of technologies that were developed during the projects.

An important target is the **Security Industry**. These companies are the natural buyers of research results that provide mechanisms and devices to monitor an environment or recognize a human being. A refined target is the **IT Security Industry,** including the **Embedded Systems Security,** the natural buyer of most cryptographic and authentication solutions. The **Telecommunication industry** is the key target of many research projects.

A number of research projects also target the **IT Integration Industry**, which is the case of all projects that in one way or another deal with policy compliance. The **Energy Sector Industry** might also be considered a potential beneficiary for all projects which focus on infrastructural threats or attacks on controller devices in critical infrastructures (SCADA systems for short), such as electricity meters.

In the broad area of the **Service Industry** two areas (**Social Network Providers, Logistics Services**) might use directly a number of techniques from the projects focusing on privacy and identity management.

Recommendation. *With the few exceptions of IT security services, in all other industries the transfer of research results to market requires mediation (security is a failure of a product). This gap might be addressed by actions that try to reach and experiment directly with final end-users.*

II. KEY RESEARCH RESULTS WITH INNOVATION POTENTIAL

A rough classification of the technical results with innovation potential can divide them into the following major classes:

- At one end of the spectrum we find results that can appeal to **product innovation in ICT for citizens**, e.g., a biometric driver authentication module (mass market). The **major obstacle for results targeting innovation for citizens is the strong force of inertia and societal acceptance issues**: it is difficult to convince millions of customers to pay a higher price for a car that cannot be easily stolen, but also cannot be lent to their friends by a simple hand-over of a key. Yet, once the results targeting product innovation in ICT for citizens are accepted, the law of inertia will play in their favour.
- An intermediate area within the innovation spectrum is the wide area of **innovative products for software developers and system administrators**. Products in this area are, e.g., an intrusion detection system (IDS). **Efforts to transform research results in this area must also overcome the hurdles of inertia**, as they need a vector for the distribution of their technology to a large (albeit not mass) market. At the same time, they must be able to maintain and adapt the technology as the underlying IT languages and systems evolve.
- At the other end of the innovation spectrum we find results which address **product or process innovation for ICT specialists**, e.g., a security protocol verification toolkit (niche market). Advocates of the products in this area must be able to tailor their products to very specific customers' needs and internal quality processes. **They face a minor inertia as the adoption of a technology is essentially a single decision**: if they can prove that the technology saves money or improves product's quality the steps to adoptions are short.

- A separate case are **knowledge-based contributions**: they do not identify a specific result that can be transformed into a product, but they are a tangible manifestation of an increased knowledge that can be concretely used by the community. Projects that produce databases of information (attacks trends, vulnerabilities etc.) belong to this category.

Product Innovation in ICT for Citizens. A report from Oxford Economics shows that the total size of digital economy in 2013 is estimated to be at $20.4 trillion, equivalent to roughly 13.8% of all sales flowing through the world economy[2]. It is a fast-growing market: only the business-to-consumer e-commerce sector (excluding travel) is expected to jump from $572 billion in 2010 to over $1 trillion by 2014. This confirms the trend predicted in the Booz&Co survey commissioned by the EU[3]. The same report points out that while the digital economy creates significant opportunities for companies, it also escalates the threat of breaches in cyber-security, misuse of intellectual property and reputational damage from open communications on the web

Among the results that have the potential to lead to product innovation in ICT for citizens, we can list:

- **Biometric technologies complementing traditional biometric recognition systems** (a blooming market with global revenues forecasted at $11 billion annually by 2017[4]). Complementary biometric technology makes use of face dynamics and activity-related actions to recognize the user when on the move, or to improve the results of traditional biometric models. It can also be used to provide an alternative way to access services by disabled people.

  FP7 projects (e.g., ACTIBIO, MOBIO and TABULA RASA) have developed an innovative car driver authentication model and a biometric authentication system for mobile devices; they have also worked to improve the reliability of biometric systems.

- Another large market that can be affected by security projects is the **domain of controller devices in critical infrastructures** (SCADA networks). Frost & Sullivan estimates it will reach $6,9M in 2016[5] (from $4.5M in 2009). Given the context in which they are employed, the vulnerability of these systems may lead to serious threats, and the consequences of a successful cyber-attack on an infrastructure of national significance are potentially dire. The need to strengthen the reliability of these systems and the increasing demand to modernize power, water and wastewater infrastructure all over the world makes this market a promising one.

  Funded projects (e.g., MICIE, INSPIRE, VIKING, SECFUTUR and MASSIF) have achieved, e.g., improving the QoS in the energy supply chain; they have developed systems for assessment of the SCADA network security by integrating information from detected intrusions and faults, and security enhancements for smart grid applications within energy distribution and control infrastructures.

- The other domain in which there is potential for the product and process innovation in ICT for citizens is the **realm of social networks and privacy protection**. In the last years the flow of personal information shared through social network platforms has increased (more than 30 billion pieces of content are shared each day), threatening the concrete realization of the European data protection principles, such as transparency, informed consent and purpose limitation[6]. Social network protection also significantly affects the Digital Agenda target of protecting children: 22% of Facebook users are minors.

---

[2] "The New Digital Economy: How It Will Transform Business", Oxford Economics, 2011

[3] "Digital Confidence. Securing the Next Wave of Digital Growth", Booz & Co., 2008

[4] "The Future of Biometrics", Acuity, Market Intelligence, 2009

[5] http://www.frost.com/prod/servlet/press-release.pag?docid=218949720

[6] http://www.graphicsms.com/blog/1710-social-network-statistics-2011/

Funded projects (e.g., PRIMELIFE and PICOS) have developed several technologies for privacy management of social network users, including an anonymous digital credential scheme, which were evaluated by a significant amount of end-users. This potential could be relaunched by the forthcoming eID European legislation.

- The **Internet of Things** can reasonably be included in this section due to his huge potential in terms of growth in revenues, users and data sharing. Indeed, Beecham Research predicts that global revenue from these objects will grow from $15 billion in 2011 to more than $30 billion in 2014[7], and, according to Cisco, by 2020 there will be 50 billion 'things' connected to the Internet[8], largely exceeding the number of people on the Earth, and as each of this sensor is potentially a point of vulnerability to exploit, new security challenges will be required to protect data and user's privacy.

  Research projects active in this field (SEPIA, TAMPRES and UTRUSTIT) focused on trustworthiness, security and protection properties of interconnected devices and networks of such devices; and provided enhancements of mobile platforms, cryptography and privacy protecting technologies, as well as the delta-evaluation and certification methodologies.

Product Innovation for System Administrators. This class of users is significantly large; and they belong to the class of technically-aware **users that could be easily targeted by owners of FP7 security and trust research results**: according to an Ernst&Young's survey 51% of respondents (information security executives) complain about the lack of a suitable protection mechanism against attacks on IT systems[9]. In the same time, Symantec reports on heavy economic consequences of cyber-attacks: in 2010 20% of small businesses lost at least $100,000, that figure is even higher for large enterprises, as 20% of them lost $271,000 or more in damage[10].

Many funded projects (e.g., PRISM, DEMONS, AWISSNET and POSECCO) have produced management and monitoring tools (e.g., an IDS based on novel traffic monitoring techniques and a monitoring infrastructure to detect security and network disruption incidents across multiple domains and jurisdictions) for complex IT systems that could be marketed by spin-off enterprises. These results have the potential to improve the overall ecosystem, but it is unclear from the evidence supplied by the projects whether there is enough economic margin for distributors.

***Recommendation**: Participation of companies (or subsidiaries) that directly market security products or offer security consultancies should be promoted.*

Product Innovation for Software Developers. "Plug-and-play" security libraries and toolkits for mainstream software and Information Systems developers were the target of many projects funded under the *Trust and Security* programme. Among the concrete results achieved by these projects (CACE, ECRYPT II, VISSENSE, TECOM WSAN4CIP and ANIKETOS are examples of projects in this area) are novel efficient implementations of secure cryptographic systems; packages for trusted operating systems and trusted protocols for embedded security-critical applications and advanced crypto-libraries for secure multi-party computations.

Product and Process Innovation for ICT Specialists. According to a World Bank report, the European ICT service export in 2011 was at $13.3 billion (balance of payments)[11]. To support this strategic advantage of the European countries in the ICT service area, the FP7 projects have developed innovative solutions in several key areas.

---

[7] http://www.adlittle.com/downloads/tx_adlprism/ADL_Smart_market-makers.pdf

[8] "The Internet of Things: How the Next Evolution of the Internet Is Changing Everything" D. Evans (Cisco), 2011

[9] "Into the Cloud, out of the Fog. Global information Security Survey", Ernst & Young, 2011

[10] "State of Security Survey", Symantec, 2011

[11] http://www.tradingeconomics.com/euro-area/ict-service-exports-bop-us-dollar-wb-data.html

- A group of funded projects focused on **information system compliance** covering the product/process innovation for ICT specialists market area of information system analysts, architects and auditors (for the system design phase).This is a **market with significant potential, as it is at the high-end of the value chain of IT system development**. Currently more than 200 firms offer risk-consultancy services; this market was estimated at $36 billion in 2011, and is expected to grow to $50 billion in the next few years. Organizations require advice on governance, risk management, and compliance (GRC) strategy, organization and process design and services to help develop and integrate GRC technology infrastructure[12]. However, this market is very fragmented and reaching it out and penetrating it would require major dissemination effort.

  The main result of the funded projects in this area (MASTER, GEMOM, SECURESCM) is typically a methodology for secure and trustworthy system design that is supported by one or more tools.

- Projects working on **specialized embedded systems security** (e.g., UAN and SEPIA) or **protocol design and verification** (e.g., AVANTSSAR, AWISSENET and TWISNET) can produce niche results, which are directly marketable, such as a sensor network working on acoustic channels for underwater surveillance, a design of secure mobile platform, or a protocol verification toolbox. Yet, it is not clear how to evaluate the potential of this market.

- Innovative products for ICT specialists in **security certification, verification and testing** are a marketplace for service certification, automatic bug-fixing tool and runtime service security testing platform delivered by ASSERT4SOA, PINCETTE and SPACIOS.

Knowledge-Based Contributions. A special category is represented by projects (e.g., INTERSECTION, SHIELDS, VIKING, and WOMBAT), which contributed some research **results that cannot be easily transformed in products, but that represent a significant contribution to some objectives of the Digital Agenda**, such as the development of databases of models of reaction of society under attack, or a world picture of current malware distribution. It is not clear how to continue to populate these data repositories with actual industry data after the project is over. A successful (if only) example, albeit limited by non-disclosure agreements, is the WINE[13] infrastructure with actual malware data, which has been taken up by Symantec as a follow-up of the WOMBAT project. The only feasible alternative seems an open-source community (but then there should be a clear value for contributors) or an individual industry take-up (where the value for the individual industry is clear).

Other Innovation Contributions. Many projects (e.g., CONSEQUENCE, INSPIRE, GEMOM, INTERSECTION, PRISM, TAS3, TURBINE, WEBSAND, etc.) produced among their results security and privacy architectures and frameworks of different kinds. **These results are the most difficult to transform into innovative products**: while an IDS system can be transformed and marketed into a product that third parties can buy, a security architecture can only be adopted within the main IT architecture. Therefore, the potential users are limited to the mainstream software integrators and producers (e.g. IBM, ATOS, SIEMENS, THALES, etc.) or public entities (that can mandate the architecture in their products). Since IT integrators have their own security architectures and the benefits of different architectures are hard to evaluate, the barriers to the market are significant for adoption outside the members of the consortium (and even within the consortium).

In many cases the projects of this category also developed a policy specification language. Some of these languages have been standardized through OASIS, but their **commercial adoption is subject to even more uncertainties** than novel IT architectures: the adoption of a policy language requires adoption of the corresponding enforcement engine, and therefore existence of a company that commits to provide an open source or a commercial engine.

---

[12] "Trends in Governance, Risk and Compliance", M. Rasmussen and C. McClean (Forrester Research), 2011

[13] "Toward a Standard Benchmark for Computer Security Research: The Worldwide Intelligence Network Environment (WINE)", T. Dumitras and D. Shou (Symantec Research Labs), at BADGERS'2011.

III. PROJECT CONTRIBUTIONS TO THE DIGITAL AGENDA

The project results were categorized by the project coordinators following the key features of the Digital Agenda objectives (the most relevant is Pillar III: Trust and Security, as identified in Action Area 2.3 of the Digital Agenda for Europe, document COM(2010) 245, with 13 specific actions numbered from 28 to 41). For the broad items (e.g. Action 54 Develop a new generation of web-based applications and services) all assessed projects contribute to this achievement.

However, **most projects are too technically-oriented to make a direct contribution fulfilling completely one of the Action items 28-41**.

- ***Actions Targeting Policies and Regulations (Actions 17, 28, 29).*** The funded projects have contributed to creating of a European Trust Observatory (an initiative towards development of trust compliance policies and procedures for service providers); designing a roadmap of best practices for the network systems and communication networks protection, that could be used to guide Telecom operators in adoption of security strategies; and supporting the working groups on SCADA and network security.
- ***Actions Aiming at Improving Knowledge of Cyber Attacks (Actions 30, 33, 39, 41).*** Several projects have worked on development of novel technologies for detection and prediction of cyber-attacks and protecting critical national infrastructures; creation of security vulnerabilities repositories and tools for cyber-attack simulations and impact analysis. In this case some of the project results provide an indirect support for these actions.
- ***Actions Focusing on Privacy (Actions 34, 35, 37).*** Albeit research projects do not work specifically on supporting the revision process of data protection legislation, they can provide technical tools for the implementation of such provisions, and also provide experience of potential problems with user adoption. This means that their results are also directly relevant to the action points in this category. Among the significant contributions in this area we can mention the end-user evaluation of privacy violations executed within the pilots carried out in the social network-focused projects; a privacy specification language; privacy implementation guidelines for Telecom operators and frameworks for implementing and monitoring compliance with the privacy legislation rules.
- ***Actions not Directly Supported by Project Results (Actions 31, 32, 36, 40).*** For these points of the Digital Agenda, there was no project result that could contribute directly to its implementation, but only indirectly to provision of results to industry and the ecosystem in general.

> ***Recommendation:*** *The project proposals on cyber-security and preparedness to counter cyber-crime and cyber- attacks and protection of children (e.g., specialized credentials or anonymity) on the Internet might be treated preferentially, as covering for the under-supported Actions. Initiatives such as Joint Calls might be an option to pursue in these sectors.*

IV. INSTRUMENTS TO FILL INNOVATION GAPS

The feedback from project coordinators also identifies gaps in the “last mile” to a product that could be addressed by a mixture of organizational, funding, and regulatory measures by the EU Union:

- **Improved use of existing instruments (by the Unit)**. Security products adoption is often obstructed by the common public perception that security is an unnecessary and expensive "extra feature". This perception problem can be addressed, for example, by public procurement contracts mandating security and privacy features in the delivered solutions.

- **New instruments for supporting trials and pilots (by DG Connect).** Existing project financing schemes rarely allow sparing some time and money on pilots with actual users; yet, pilots can be crucial for transferring an innovative technology into a commercial solution. In the future pilots and user trials may be funded through a novel competitive scheme available to successful projects.
- **A new regulatory disclosure initiative (by the EU as a whole).** Lack of shared data on actual attacks and vulnerabilities in IT systems hinders evaluation of security research results applicability to the real world problems. An EU-wide legislation to mandate sharing of this data will improve validation of security solutions and ameliorate resilience of the public and private infrastructure to cyber-attacks.

Gaps to be Filled by Improved Use of Existing Instruments. The first problem raised by project coordinators is the **lack of perception by large parts of governments and the IT industry that security is a major, if not critical, issue** that can make the difference in the market: from a business point of view indeed a higher request of security products tallies with major interests and investments in the R&D sector. Also in the realm of privacy the most important problem is the perception of privacy features by operators. When a research result concerns privacy, especially in network monitoring, the actual implementation of privacy-protecting measures is always perceived as an extra cost. Therefore it is difficult to convince operators to adopt or even to pilot solutions whose goal is to better protect the privacy of the customers.

To this extent the role of governments and public entities could be not only to mandate the usage of privacy features and security protection mechanisms in private corporations, but also to adopt the innovative features for their own benefit. Public procurement contracts are a significant market, and making security and privacy features mandatory in those contracts might tilt the perception of security and privacy as a cost into an added value, making the difference in a securing a bid.

> ***Recommendation:*** *The existing instrument of pre-commercial procurement should be used and further promoted to create long term pilots supported by public administrations.*

Another issue that emerged was the **lack of structured and documented relations with product groups within the industry partners**. Each project had a number of industry partners that provided requirements, case studies, scenarios validation, and eventually implemented some solutions. These activities are well described in the deliverables of the projects; however, they were carried mostly by the research arm of the industry partner. Only few projects pointed to a deliverable, where a structured relation with product groups (e.g., a user trial) is described.

In most cases the relation with the product group is managed internally with the industrial partner and it is not project-wide. Occasionally the product groups are very interested in what the project is doing and there is a regular exchange of ideas and commitments, even though the relation is often not structured and not precisely defined: a non-functional mismatch could be encountered if the relation is not established from the very beginning of the project, and this could become an issue to the final exploitation of the results. It is not clear if setting a structured relationship with the product group from the very start of the project lifetime could be functional or could become a bureaucratic hurdle that will stifle innovation. Yet, offering visibility of such trials could be beneficial for the community. What is clear is that **obtaining early feedback from the product groups during the lifetime of the projects might actually help to shorten the path from research to innovation**.

> ***Recommendation:*** *Results of product group trials should be reported appropriately in the same way as user trials (if any). Obviously, some results of the pilots would not be public for IPR reasons, but lessons learned should be visible, as it happens in medical trials.*

New Instruments for Supporting Trials and Pilots. We often need to weave the security solution into a "normal" application, or to "adapt" the base system of the final target beneficiaries in order to accommodate the solution. An example: nobody buys a flexible privacy policy as such, but people might buy a social network with a flexible privacy policy if it improves user experience. The main idea might be really interesting, but the **technical gaps in the target (non-security) system may require additional efforts in order to be tried out**. For example, accessing a web system with facial biometrics instead of passwords requires a high resolution webcam to be present on the client system. Notice that we are not speaking here of the additional effort needed in order to transform research results into fully-fledged products, but of the effort that is needed to have a fully-fledged pilot system.

Carrying out a pilot requires an additional effort that cannot usually be made within the timeframe and the resources of the research project for two reasons. Firstly, this gap is not interesting from the viewpoint of research or technological development; it will not increase the project rating by the reviewers, nor the research standing of the academics participating in the project. Secondly, but most important, it requires a significant effort for systems integration at the operational level that can only be realistically carried out after research results have been completed and validated.

Occasionally some projects "continue" the work with a strand dedicated to more detailed experiments in a new research project. **This line of action is sub-optimal from the viewpoint of innovation**. Firstly, they are "new" projects and thus subject to all hurdles in the evaluation, as if they were never reviewed before; and secondly, being "research" projects the majority of effort needs to go into developing new research (rather than bridging the gap with user trials). Most project coordinators suggested that new instruments should be tried, as the current ones could not be effective.

> ***Recommendation**: A specific instrument might be introduced that would still comply with pre-competitive requirements: a competitive call available to a subset of partners from concluded or near completion projects; with a narrow focus (a large-scale user trial of a result from a research project); simplified along the calls for international cooperation or enlargement to partners from new member states.*

A New Regulatory Disclosure Initiative. All project coordinators agreed that a **major problem in the innovation path is the secretive approach to disclosure of security problems** in industry and commerce. Without benchmarking data it is difficult to evaluate whether a research result it is actually able to make a difference in reality.

Also in the case of critical infrastructures, all project coordinators noted the **unwillingness of operators to disclose and to share information about their infrastructure, and about attacks against their networks**. This was also true for telecom operators and service providers. Such reticence across industries is clearly not only due to the need to protect the infrastructure. Disclosing statistics or research-level information on vulnerabilities or detected attacks on the infrastructure does not allow other attackers to replicate an attack or exploit a vulnerability, because a huge amount of low level and operational information would also need to be disclosed in order for an exploit to be possible.

This phenomenon can be attributed to the perceived risk of liabilities and reputation losses if the presence of security problems is admitted. Most project coordinators and technical leaders noted that this could only be solved by regulatory initiatives, and we agree.

> ***Recommendation:** A European-wide regulatory initiative is required to mandate the controlled disclosure of security incidents, along the lines of what is happens in the air traffic management.*

V. CONCLUSIONS

In this paper we have reported on the FP7 ICT Trust & Security Programme projects' innovative contributions and their perspectives of commercialization. The study of the projects' results was carried out by the University of Trento with support of the Effects+ partners. Our conclusions are grounded on the projects' documentation analysis and the ethnographic study (including a series of focused interviews) with projects' officers, coordinators and technical leaders. A parallel analysis based on the projects' documentation and feedback from the project coordinators was conducted to evaluate the projects' contributions to the Digital Agenda goals.

The analysis of the constituency revealed a dynamic, collaborative environment with few major players, but without clear market dominance. A variety of companies representing the software industry, the telecommunication sector, and proper security services participate in the research projects.

The study of the innovation potential identified many research results, which can stimulate product, service and process innovation in Europe. Some projects have clear innovative results that are usable by citizens (e.g., in the realms of biometrics and privacy) and IT industries (for example, in the realm of security and compliance of infrastructures). Many projects also delivered important potential innovations in tools and methods for ICT specialists (from consultants on IT governance to IT administrators). These results have the potential to be used well beyond the consortia that produced them, albeit the path to commercial products might be fraught with difficulties.

Additional details can be found in the Effects+ deliverable D2.2 "The innovation potential of FP7 ICT Trust & Security projects".

Based on the study results and the project coordinators' feedback we have identified some recommendations for the European Commission for further strengthening of the EU ICT Security industry. They are presented at the beginning of this paper.