EFFECTS+ Clustering of Trust and Security Research Projects, Identifying Results, Impact and Future Research Roadmap Topics

Frances CLEARY[1], Keith HOWKER[2] , Fabio MASSACCI[3] , Nick WAINWRIGHT[4],
Nick PAPANIKOLAOU[5] , Michele BEZZI[6] , Pedro SORIA RODRIGUEZ[7]

[1,2]*Waterford Institute of Technology - TSSG, Carriganore, Cork Rd, Waterford*
Tel: +35351302919, Email: fcleary@tssg.org, khowker@tssg.org
[3]*Universita Degli Studi Di Trento, Italy*
Email: Fabio.Massacci@unitn.it
[4,5]*HP Labs, Bristol, UK*
Email: nick.wainwright@hp.com, nick.papanikolaou@hp.com
[6]*SAP AG, Germany*
Email: michele.bezzi@sap.com
[7]*ATOS, Spain*
Email: pedro.soria@atosresearch.eu

Abstract: Structured and coordinated clustering increases the effectiveness of R&D project work helping to raise awareness, align approaches and create synergies. The project EFFECTS+ coordinates such clustering and trust and security research project potential impact analysis activities. This provides the wider community with an interest in the trust and security research space the opportunity to participate, contribute to and gain an overall view of current state of the art and active research projects ongoing within the Europe in this domain. This paper will provide you with an overview of the activities completed by EFFECTS+ to date, highlighting the clustering structure and the research project impact analysis completed so far. EFFECTS+ also focuses on the development of a trust and security strategic research agenda for future work. This paper will address the process and structure adopted by EFFECTS+ for the identification and consolidation of such future roadmapping content.

1. Introduction

Dissemination, networking and striving to create synergies and collaborations is a key element for any current research project. EFFECTS+ [1] an FP7 funded coordination and support action operates with this main objective in mind by working to support clustering amongst FP7 ICT trust and security projects, highlighting research achievements coming from such ongoing innovative research, landscaping their results and identifying future research roadmap for this trust and security domain. Project clustering provides passive awareness of parallel activities, enabling active collaboration and cross-stimulation at the programme, project and personal levels as well as providing for improved dissemination of research results in this field, and input into the agenda and roadmaps for future research. There is a growing community of researchers and developers involved in addressing what needs to happen to the Internet and its dependants with respect to the wide range of R&D challenges concerning Trustworthy ICT, including security, trust, privacy, dependability. Questions arise about the resultant trustworthiness of the system as a whole: in particular, how do we ensure and validate that when the basic technical challenges are met and products and services become available, that the various elements work together as expected; that they conform to specification; and that they comply at the design and operational stages with the architectural and regulatory standards and requirements. Framework Programme (FP) projects are seeking solutions to many of the identified concerns. EFFECTS+ helps to provide an overview of the current research ongoing in this area, highlighting the main topics being addressed currently, the potential impact of such results and future research roadmap in this domain. This paper will address the following main topics, expanding on the clustering, analysis and roadmapping activities completed within the EFFECTS+ project, highlighting various recommendations coming from each activity:

- It provides an overview of the EFFECTS+ clustering activities, highlighting the methodology used to identify the specific clusters. Discussing the individual cluster groups, and the main topics prioritised in such clusters.
- It summarises and details the main topical achievements of security, trust and identity projects from EU FP Call 1 and Call 5.
- It provides a summary of recommendations from the EFFECTS+ analysis of trust and security research projects in the current Framework Programme.
- It identifies the main research gaps, issues and topics identified in the EFFECTS+ trust and security research roadmap.

1. Trust and Security Research Project Clustering

Supporting project collaboration via content-related technically focused clustering works to enhance interoperability and leverage synergies between projects. Benefits for involvement in clustering activities vary and include:

1. Promotion of achievements of current trust and security projects amongst the clusters;
2. Improved networking amongst experienced researchers in this domain;
3. Positioning that allows monitoring of research projects within the Future Internet Assembly – working to articulate their inputs.
4. Limiting the duplication of work at European and national level via dissemination of ongoing research to a wider audience.

1.1 Landscape of FP7 project results - Methodology

A suitable structure and methodology to identify such relevant cluster themes completed by EFFECTS+ [2] and involved ethnographic studies of current projects with the outcome being a first proposal for a cluster structure, with further refinement of this structure following an initial feedback session and meeting with the project representatives. Two main dimensions for FP7 project classification were identified to support the methodology and process, these included ‘*Abstraction level of the target research’* for example a distinction between IP networks and web services. Table 1 highlights the various abstraction levels considered. This level represents an appropriate clustering dimension, and most projects can position themselves in one or two classes. ‘*Result Type’ (Provisioning v’s Assessment distinction*) was the second dimension taken into account. This dimension looks towards the expected outcome of the project for example results of a provisioning project could be a new security service (e.g. new authentication method) or the results of an assessment project could be a tool that establishes the security level of a service e.g. verification mechanism for authentication, as per table 2 .

Topics Covered	Abstraction Level
Business processes	⇓ ⇓
Web services	Clouds & Services
Middleware	⇓ ⇑ ⇓
Operating system	⇑ ⇓ ⇑
Networks	Systems & Networks
Hardware	⇑ ⇑

Table 1. Abstraction Levels.

Topics Covered	Result Type
Security primitives and protocols	⇓ ⇓
Security services	Provisioning of Security Services
Monitoring services	⇓ ⇑ ⇓
Security verification and assessment	⇑ ⇓ ⇑
Security design methods	Assessment of Security Services
Security Intelligence	⇑ ⇑

Table 2. Security Provisioning vs. Security assessment.

Supporting the cluster identification methodology a supporting process was also adopted and implemented this included, obtaining abstracts of projects from CORDIS and the completion of a preliminary analysis of the activities based on this source of information as well as referencing the individual project websites and publicly available deliverables. Completing interviews with project coordinators and technical and scientific directors. Then in turn interviewees reviewed the result of the interview and provided feedback.

1.2 Trust and Security Cluster Setup

Coming from the initial landscape and ethnographic analysis phase, three trust and security clustering groups were set up (see Figure 1):

- Systems and networks (technical cluster) – covering topics like Assurance, Policy, Trust, secure service composition, semantics/ontology, security metrics, privacy.
- Services and cloud (technical cluster) – covering topics like Privacy in SIEM, attack models, trusted computing, security by design (H/W) , critical infrastructures.
- Networking and coordination (non-technical cluster) – covering topics like identify synergies, scoping activities together, calendar coordination/alignments, outreach to other units/initiatives.

These clustering groups have been active , with dedicated cluster events, workshops and a specific Cyber security and privacy EU Forum 2012 conference (April 2012) [3]. Future clustering activities can be viewed at the EFFECTS+ website [1].

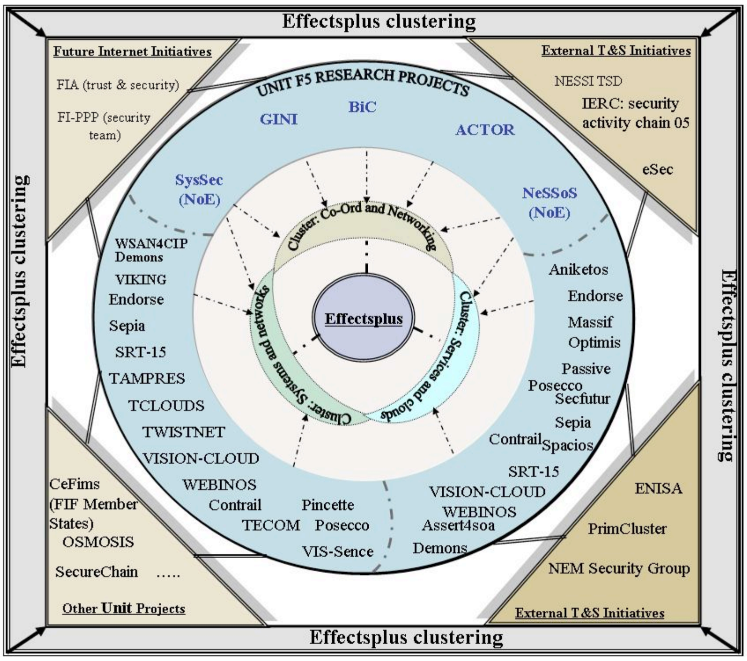


Figure 1. EFFECTS+ clustering structure.

2. Innovation Potential of FP7 Security and Trust Projects

A comprehensive study on the innovation potential of FP7 T&S projects funded by ICT Call1 for trustworthy ICT and the joint ICT and security call was completed within EFFECTS+ [4]. Such a study was based on documental evidence (deliverables, publishable reports, etc.) and an ethnographic research (interviews and feedback from project coordinators). The security market represents a rapidly growing sector. The Impact of the current T&S research projects needs to be highlighted with the question being posed Do security and trust FP7 projects have some key results that could contribute to this market demand?

The analysis of the ***industrial landscape*** showed a connected community (a scale-free network) with few major players, but without a clear market dominance:

- few general *software producers and integrators* act as bridges and hubs between different interests groups (such as privacy and critical infrastructure protection);
- *specialized IT security companies* are emerging as actors involved in two or more projects, but are still at SME stage.

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.

The study of the ***innovation potential*** identified many research results which can stimulate product, service and process innovation in Europe. In synthesis:

- some projects have produced research *results that are directly usable by citizens* (for example in the realms of biometrics and privacy);
- most projects have delivered significant innovations in *tools and methods for ICT specialists* (from consultants on IT governance to IT administrators) that are widely usable beyond the project's consortium. Such contribution is mostly in the area of command, control and compliance (of networks and IT systems).

An interesting contribution by some research projects is represent by an improved *community knowledge* of the security echo-system. This knowledge can be used by decision makers to shape their agenda.

The Security and Trust projects also contributed to the ***achievement of the objectives of the Digital Agenda***, in particular on those focusing on instruments for self-regulation and for improving privacy and security of infrastructures and services.

The analysis also showed that two major issues are only addressed partially and indirectly by the projects of Call 1, Call5 and the joint Security and ICT Security Call::

- *cyber-security and -preparedness to counter cyber-crime and cyber- attacks*
- *children protection on the internet*

Initiatives such as Joint Calls might be an option to pursue in these sectors.

The analysis also identified gaps in the "last mile" to a product that could be addressed by a mixture of organizational, funding, and regulatory measures such as

- set-up of *structured relations with product groups or users* from the project's start,
- specific *funding measures by the EC for experimenting in large scale trials* with a simplified funding procedure,
- European *regulatory initiatives on the controlled disclosure of security incidents*.

The adoption of these measures might ensure that ICT progress is rapidly transformed into products for the benefits for Europe's citizens, businesses, industry and governments.

3. Trust and Security Research Roadmap

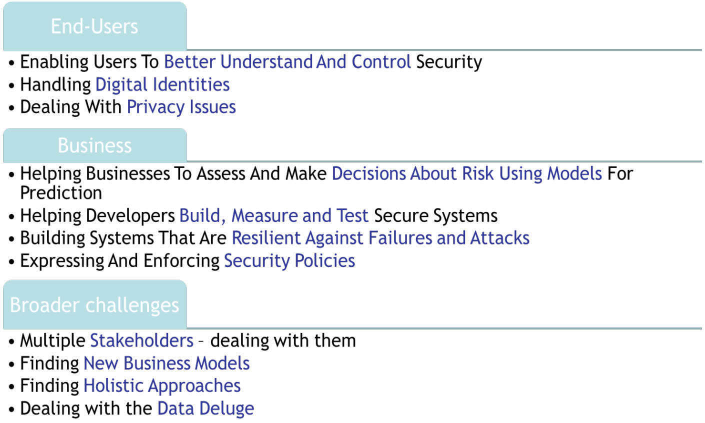
EFFECTS+ has worked with the Trust and Security research community to develop a research roadmap with the intention of identifying key topics and approaches that require further research in the timeframe of Framework 8, i.e. for research in the 2014-2020 timeframe with potential for impact in the mid-long term.

3.1 Research Roadmap Structure and Process

Key questions were asked to leading experts in this field and to the participants of the T&S clustering groups as an initial source of information and contribution to such a research roadmap. Such questions were as follows:
What are significant changes between now and 2020+ that impact this topic area? What are the drivers of this change? What is your vision for 2020+ in this topic/area? How will we make a difference? What are the hard challenges, big gaps, what will be difficult, what are the significant barriers to achieving this vision? What radical approaches, disruptive technologies, new ideas might be solutions to these challenges?

The output 1st draft report titled "Trust and Security in the Future Internet: Setting the Context" identified challenges and potential solutions, societal shifts and changes of relevance, and a vision for the future of the trust and security field.
Various challenges that were perceived as having an impact on the field were grouped under the following rubrics (see Figure 2):

- Changes in the way end users (citizens) perceive the role of the Internet in their lives and use it on a day-to-day basis,
- Changes in the way business is conducted, and how different sectors are being affected by developments in technology, and
- Changes in the broader socio-economic landscape.



End-Users

- Enabling Users To Better Understand And Control Security
- Handling Digital Identities
- Dealing With Privacy Issues

Business

- Helping Businesses To Assess And Make Decisions About Risk Using Models For Prediction
- Helping Developers Build, Measure and Test Secure Systems
- Building Systems That Are Resilient Against Failures and Attacks
- Expressing And Enforcing Security Policies

Broader challenges

- Multiple Stakeholders - dealing with them
- Finding New Business Models
- Finding Holistic Approaches
- Dealing with the Data Deluge

Figure 2. Research challenges identified for three target groups.

4. Potential Solutions for Trust and Security in the Future Internet

Following the identification of challenges (figure 2), this section will highlight some of the approaches that may be considered in order to tackle such future internet issues and challenges.

3.1 Solutions for Users of the Future Internet

End users strive to gain more control over their active digital lives. The digital wave has brought more devices and applications and the need to customize and have control over your digital experience, is an increasing requirement from end users. To help address this issue potential solutions could include

- Development of universally acceptable digital identifiers
- Education of Citizens (raise awareness of security and privacy risks)

3.2 Solutions for the Enterprise

Many tools and techniques could potentially be used more effectively, enabling businesses to be more success in their future ventures. Examples of such solutions to challenges addressed in figure 2 could be for example

- Better Languages and Tools for specifying secure software
- Improve assurance methods
- Privacy-aware software development
- Development of rich and expressive security models
- Development of tools for tracking data

3.3 A Vision for Society and the Wider Economy

More international collaboration is required to address the main challenges that exist. Such collaboration is essential when dealing with security related matters, as much cybercrime transcends national barriers.

- Cooperation on issues of national security
- Enhancement of legislation to accommodate technological development
- Research and investment in security tools and technology
- Consideration of novel, radical approaches.

5. Conclusions

EFFECTS+ continues with its clustering, analysis and roadmapping activities, maturing the content and outputs coming from the projects objectives over time. Clustering remains a core objective and activity of the EFFECTS+ project, with an endless quest to work to increase collaboration and dissemination of project results and strive to create synergies amongst projects, experts, industry and policy makers in the trust and security domain, maximising the impact of the research activities active within this space.

From the initial landscape and project innovation potential analysis a number of recommendations have been drawn up, in an attempt to highlight recommendations that can be used to strive to improve the impact coming from active research projects.

Such recommendations [4] include the following:

Recommendation 1. Projects should report in more effective and consistent way the methodology and actual dimension of pilots and trials with end users or product groups.

Recommendation 2. use and promote the existing instrument of pre-commercial procurement to create long term pilots supported by public administrations.

Recommendation 3. Push projects to establish a structured and visible relations with products group of the companies within the consortium from the very start. Results of product groups trials should then be reported appropriately in the same way user trials (if any) are reported. Obviously, some results of the pilots would not be public for IPR reasons, but lessons learned should be visible. It is of course difficult for a product group to buy in advance a story line such as "we have this great, vague, idea that in a couple of years will be prototyped!" typically the real discussion starts when you have something to show..." The objective of an early and progressive engagement is to understand the actual needs which might later lead to a prototype that actually addresses some those need.

Recommendation 4. A European-wide regulatory initiative is necessary to mandate the controlled disclosure of security incidents in the same fashion of what happens for safety in avionics.

EFFECTS+ trust and security roadmapping activity is still currently ongoing and is working to mature and expand on the current input already in existence, going into further details on the challenges and potential solutions for the three main identified focus groups (i.e. end users, enterprise, society and the wider economy). This T&S research roadmap will also feed into the future internet Assembly Research Roadmap for the Future internet[5]. This is an important activity, to help promote the importance and need for research in this domain to continue, now more than ever in this digital era.

References

1. http://www.effectsplus.eu/
2. EFFECTS+ Deliverable D2.1: Results and Impacts of FP7 projects http://www.effectsplus.eu/files/2012/04/D2.1-Results-and-Impacts-of-FP7-projects.pdf
3. http://www.cspforum.eu/
4. EFFECTS+ Deliverable D2.2: The innovation potential of FP7 security and trust projects (Draft Version 1) http://www.effectsplus.eu/files/2012/04/D2.2innovation-Report-Call1_V1.pdf
5. http://fisa.future-internet.eu/index.php/FIA_Research_Roadmap