Research and Innovation Impact of Trust & Security Programme

White Paper 2013

Fabio Massacci, Olga Gadyatskaya (University of Trento)
Frances Cleary (Waterford Institute of Technology)

Version 1.1
October 2013

Executive Summary

This white paper is a summary of key findings on the emerging issues of the Research and Innovation Yearbook 2013 produced by WP3 of the SecCord project. The aim of the Yearbook is to investigate the R&D projects executed under Trust & Security (T&S) Programme and present the discoveries of the study conducted with the project leaders to key stakeholders.

For this white paper we have identified two emerging issues to be presented in more details: the *NIS Platform initiative* and the *status of the EU ICT security domain* as reported by the interviewed R&D project leaders.

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 Nº 316622 (http://www.seccord.eu).

Key Finding from Trust & Security Programme Analysis Executed in the Yearbook 2013

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 funded T&S research projects are capable of providing expert contributions to the NIS Platform initiative proposed recently by the European Commission. The NIS Platform is an instrument that will work to improve the EU cybersecurity status. In this white paper we list the projects that have gained expertise and developed technologies in the domains currently defined in the NIS Platform:

- risk management and security awareness promotion in organizations;
- threats information exchange across organizations;
- roadmapping for secure ICT research and innovation.

The EU R&D projects produce results that have potential to be utilised 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. Industry players from these domains participate in many of the R&D projects as validation experts and actively seek to identify and adopt delivered technologies with high market potential.

Interviewed project participants actively shared their opinions on the status of the EU ICT Security domain. The interviewees reported their views, highlighting gaps in the industrial acceptance of the technologies delivered by research projects, and suggested addressing 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.

More information on the Trust & Security Programme and the details of our findings can be found in the Research and Innovation Yearbook 2013 of SecCord.

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 greatly advanced the state of the art in this domain. Moreover, the EU policy makers and coordination bodies (such as the Network and Information Security Platform) can use these results and expertise to gain insights on the technological as well as social, economical and legal challenges in the strategic EU activities. In this section we list the T&S projects whose experience and innovative contributions are the most relevant to the identified security and trust challenges ahead of the NIS Platform (in Table 1).

The NIS Platform comprises three Working Groups[1]:

- *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 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 T&S research projects from Call 1 and Call 5 are over or close to completion; 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.

From the T&S research project to NIS Platform mapping, we can see in Table 1 that WG3 can enjoy contributions from the largest share of projects. Also WG1 can receive a rich input from the EU Trust & Security projects. Instead the WG2: Information exchange has fewer projects that have contributed to its goals, most of them from Call 1 and Joint ICT-SEC Call.

Notice that Table 1 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 1 Projects that can contribute to the goals of the NIS Platform 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	**MASSIF**: a SIEM framework for scalable multi-level event processing and predictive security monitoring	**CYSPA**: a methodology to evaluate an impact of cyber-disruptions on an organization

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

	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	**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 patterns in network infrastructure	**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-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-	**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	**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

	consumers in the area of secure, trustworthy and dependable ICT	future research directions **NESSOS**: a Network of Excellence in the services and systems security engineering that coordinates activities in this area **SYSSEC**: a Network of Excellence in the Systems Security domain that creates a research roadmap in this area	and development of roadmaps in key sub-areas **SECCORD**: coordination and clustering of the EU Trust & Security projects, and providing an outlook on the emerging T&S issues **STREWS**: a roadmap for future research and standardization for Web security

Status of 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 also to highlight potential strengths and weaknesses of the EU ICT security market. 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).

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 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 CSP Forum (SecCord) website[2]). 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.

[2] https://www.cspforum.eu/projects

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. This highlighted issue also proved to be very relevant also to the EU Trust & Security projects; with it being addressed via the selected projects coming from Call 8;however further steps in these directions are required.

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.