UNIVERSITÀ DEGLI STUDI
DI TRENTO

SecCord

Contributions of the FP7 Trust & Security projects towards the EU Cybersecurity Strategy

M. de Gramatica, F. Massacci,
University of Trento, October 2015

SEVENTH FRAMEWORK
PROGRAMME

Contributions of the FP7 Trust & Security projects
towards the EU Cybersecurity Strategy
Version I, October 2015

The authors would like to thank the coordinators and technical leaders of the EU FP7 Research projects on Security and Trust mentioned in this report for providing information on their research results and their potential impact.
We thank Olga Gadyatskaya and Anna Pasquali for the previous work conducted within SecCord project.

Department of Information Engineering and Computer Science
University of Trento
Martina de Gramatica - martina.degramatica@unitn.it
Prof. Fabio Massacci - fabio.massacci@unitn.it
Via Sommarive 5, 38123 Trento, Italy
tel: +39.0461.282086
fax: +39.0461.283166
https://securitylab.disi.unitn.it/

This document is the Annex D of D 3.3 “Research and Innovation Yearbook 2015” for the SecCord Project.
The research leading to these results has received funding from the European Union Seventh Framework Programme (FP7/2007-2013) under the grant agreement n° 316622 SECCORD.

For more info on Seccord Project visit
http://www.seccord.eu/
http://www.cspforum.eu/

Contributions of the FP7 Trust & Security projects towards the EU Cybersecurity Strategy

Executive Summary

The aim of this Whitepaper is to provide insights on the key results of the R&D projects executed under Trust & Security (T&S) Programme and analyzed in the Research and Innovation Yearbook 2015 produced by WP3 of the SecCord project in collaboration with the project partners. In particular, we consider these innovative project achievements as relevant contributions to the implementation of the EU Cybersecurity Strategy and its complementary NIS Directive proposal.

On the basis of previous research conducted in SecCord, we have identified how some FP7 T&S projects support with their results the objectives and the statements expressed by the above mentioned EU policy documents and how, by doing this, we can conclude that the FP7 T&S Programme has properly and substantially embraced and addressed the recommendations and intentions of European Commission moving to a more open, secure and competitive internet environment.

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

Introduction

European citizens place high expectations on ICT and related infrastructures to support and drive quality of life and economic growth, which create a dependency on the proper functioning and security of these infrastructures. Understanding the risks and threats that ICT is exposed to requires a conscious, concerted international and multidisciplinary effort that spans policy, industry and research domains. The need for this effort is not new but it becomes increasingly urgent in the light of emerging cyberspace technologies, new and more sophisticated threat agents, and the growing number of people connected and the interconnectedness of today´s critical infrastructures.

It is widely known that the growing threat posed by cybercrime has a very negative implications also for both national and international economic stability. According to [BIS, 2014] the cost of breaches nearly doubled in 2013 in UK alone and some security incidents had so severe consequences that 10% of organizations that suffered a breach in 2013 had to change the nature of their business. With an annual cost to the global economy estimated over $400 billion[1], it is clear that a high level, shared and common cybersecurity strategy would be essential to ensure prosperity and freedom and to keep the European online economy running, boosting growth and jobs.

Within this context, effective and meaningful cooperation between public and private sector is becoming increasingly unavoidable in the development of cyber security policies and in preventing and resolving cyber incidents. Very often, national internal security is dependent on the private sector's infrastructure and resources. At the same time nevertheless, the state can assist vital service providers and national critical information infrastructure as a coordinator of various interests.

In 2013, the European Commission and the High Representative of the Union for Foreign Affairs and Security Policy announced a Cybersecurity Strategy and a complementary proposal for a Directive ensuring a high common level measures to enhance cyber security across the EU. This new EU Cybersecurity Strategy is expected to lead various efforts in EU cybersecurity space, including research and innovation. Within this context, research is considered embracing a comprehensive approach, targeting not only the scientific excellence, but also fostering industry competitiveness and benefitting also on cyberspace users' and citizens' security and safety.

The FP7 ICT Trust&Security Programme has been thought to "*implement the EU Cybersecurity Strategy and to address the technological and industrial issues that derive from the Network and Information Security (NIS) policy of DG CONNECT, including the implementation of research and innovation agenda related to cybersecurity, privacy and trustworthy ICT*"[2]. Throughout the last years, significant investment has been made on cybersecurity research. According to our estimate, Call 1, 5, 8 and 10 have been funded with more than 351 M€ under FP7 from 2008[3]. This takes place against a background of unprecedented focus on cybersecurity and increasing instances of major security flaws and cyberattacks towards new security challenges.

The aim of this Whitepaper is to show the relation between some FP7 project results and the main issues raised by the EU Cybersecurity Strategy.

This report is structured as follows. We start briefly presenting the main content of the EU Cybersecurity Strategy and the NIS Directive proposal at a high level and then we proceed explaining the clustering activity performed in previous SecCord research. This document indeed follows a clustering exercise performed within a series of workshops organized by SecCord-CSP EU Forum[4] in collaboration with several European initiatives. From this clustering activities a number of keywords have been extrapolated and used to map the FP7 projects to the main challenges posed by the EU document. We decided to focus mainly on projects funded under Calls 8 and 10, but reference also to Call 1 and 5 is done when needed[5].

1 http://www.scl.org/site.aspx?i=ed39127

2 https://ec.europa.eu/dgs/connect/en/content/cybersecurity-strategy-european-union

3 SECCORD D3.3 – Annex 2 "FP7 ICT Trust & Security Projects Handbook"

4 These CSP EU Forums are fully integrated with other European research initiatives (NIS Platform WG3, CAPITAL, PRIPARE, and CYSPA projects, Annual Privacy Forum, and Internet-of-Things Week.

5 The projects cited are shown in Appendix A.

1. EU Cybersecurity Strategy

The Directive on Network and Information Security (hereinafter NIS), originally proposed by the European Commission in February 2013 and approved by the European Parliament in March 2014, is part of the European Union's Cyber Security Strategy released in 2013 and aimed at making the EU's online environment more secure and reliable. The Directive aims at tackling security related risks and incidents across the EU, imposing a minimum set of high common new security measures, both for public and private sectors across the Member States, and a series of new incidents reporting requirements.

The EU's Cyber security Strategy presents the overall vision of the European Union on how to improve, properly prevent and respond to the growing threat generated by cyber-attacks and disruptions. The Strategy is grounded on the self-evident issue that information systems can be affected by security incidents that may include human mistakes, natural events, technical failures or malicious attacks and that they are increasing in terms of severity and frequency, becoming more complex, sophisticated and transnational. Such state of affairs threaten the European values of democracy and collaboration, and the growth of the digital economy. The opening of the Strategy itself claims that: "*For cyberspace to remain open and free, the same norms, principles and values that the EU upholds offline, should also apply online*"[6].

The EU's Cyber security Strategy priorities include in particular the following pillar actions:

"**Achieving cyber resilience**: by increasing capabilities, preparedness, cooperation, information exchange and awareness in the field of Network and Information Security, for the public and private sectors and at national and EU level;

Drastically reducing cybercrime by strengthening the expertise of those in charge of investigating and prosecuting it, by adopting a more coordinated approach between Law Enforcement Agencies across the Union, and by enhancing cooperation with other actors;

Developing an EU Cyber Defence Policy and capabilities in the framework of the Common Security and Defence Policy;

Fostering the industrial and technological resources required to benefit from the Digital Single Market. This will help stimulate the emergence of a European industry and market for secure ICT; it will contribute to the growth and competitiveness of the EU economy; and it will increase the public and private spending on cybersecurity (R&D);

Enhancing the EU's international cyberspace policy to promote EU core values, to define norms for responsible behavior, to advocate the application of existing international law in cyberspace and to assist countries outside the EU in building cybersecurity capacity"[7].

The proposed NIS Directive is a key component of this Strategy. It introduces a number of measures to enhance cybersecurity, including:

New national and cooperative strategy: concrete policy and regulatory measures will be developed and implemented in the national strategy of the Member States, with the aim to maintain a minimum level of network and information security. Moreover, the EU Member States are required to appoint a national competent authority to monitor and ensure the consistent application of the Directive and to establish a computer emergency response team (CERT), responsible for handling risks and incidents.

Co-operation network: the European Commission and the competent authorities in the Member States will form a cooperation network group, both at a policy and at an operational level to coordinate against risks and incidents affecting network and information systems. These network groups will exchange information between authorities.

Security requirements: one of the priority of NIS lays in the data sharing and attacks notification process, directly handled by the Member States. Operators of critical infrastructure (energy, transport, banking,

6 http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf

7 https://ec.europa.eu/digital-agenda/en/news/communication-cybersecurity-strategy-european-union-%E2%80%93-open-safe-and-secure-cyberspace

healthcare), key Internet enablers (e-commerce platforms, social networks, etc) and public administrations are requested to take appropriate technical and organizational measures to face the security risks related to networks and information systems, preventing and minimizing the impact of security incidents affecting the core services they provide. These subjects must also notify the competent authority of incidents having a significant impact on the continuity of these services.

Use of standards: Member States are encouraged to use NIS standards for the implementation of the security requirements.

Enforcement: The national competent authorities have powers to investigate cases of non-compliance within the NIS Directive, reporting criminal incidents to law enforcement authorities.

Following the full legislative procedure, the proposal for the NIS Directive passed to the EU's Council of Ministers for a close examination. Despite the widespread acknowledgment that better frameworks for cyber security are required, some points of disagreements have been identified in respect to the EU Commission and EU Parliament proposal. The Council recently released a document outlining its own position in preparation for the informal trilogue that will be held in April 2015. Once finalized the agreed wording, the Directive will eventually come into force in 2018 and the EU countries will have to implement it into their national law.

2. FP7 ICT projects support EU Cybersecurity Strategy

The EU FP7 ICT Programme contains specific objectives[8] for trustworthy ICT as well as for combating cyber-crime, which are in line with the EU Cybersecurity Strategy. The same can be said for the H2020 Programme, launched in 2014. R&D can support security innovations related to emerging ICT technologies and foster solutions for end-to-end secure ICT systems, services and applications. Innovative results from R&D can also boost the internal market and reduce European dependence on foreign technologies, working to fill the technology gaps in ICT security and prepare for the next generation of security challenges.

The research community actively participate to the implementation of the EU Cybersecurity Strategy priorities by developing innovative, reliable and usable technological solutions to ensure more security into the ICT systems, providing contributions to standards and certifications and building more and more comprehensive frameworks to understand the cyber risk.

The aim of this Whitepaper is to show how the research results of some FP7 Trust&Security projects address to the EU's Cyber security Strategy and the NIS Directive priorities.

A clustering exercise involving 43 EU projects participating in EU research projects has identified a set of keywords extracted from EU Cyber security Strategy and the NIS Directive documents (for more details see [Compagna et al., 2014]). Authors took the five mentioned Cybersecurity objectives of EU cybersecurity strategy, and for each of them they extracted a set of keywords (Fig.1). These labels do not correspond to the categories typically used in the research community (e.g., there are security technologies/mechanisms as cryptography) and could be better described as the cybersecurity challenges and/or policy-level abstractions.

In this Whitepaper, we have tried to position some FP7 T&S projects as example within these EU objectives; the analysis will show that the projects considered do not totally cover all the five Cyber security objectives identified, but tend to focus only on some of them. In particular, most of the considered projects worked in order to provide enhanced tools, methodologies and approaches for the cyber resilience, innovative tools to reduce cybercrime and the collaborative and cooperative monitoring systems for a more secure cyber environment.

This research then provides general insights and considerations on how the research projects analyzed target the EU Cybersecurity strategic objectives.

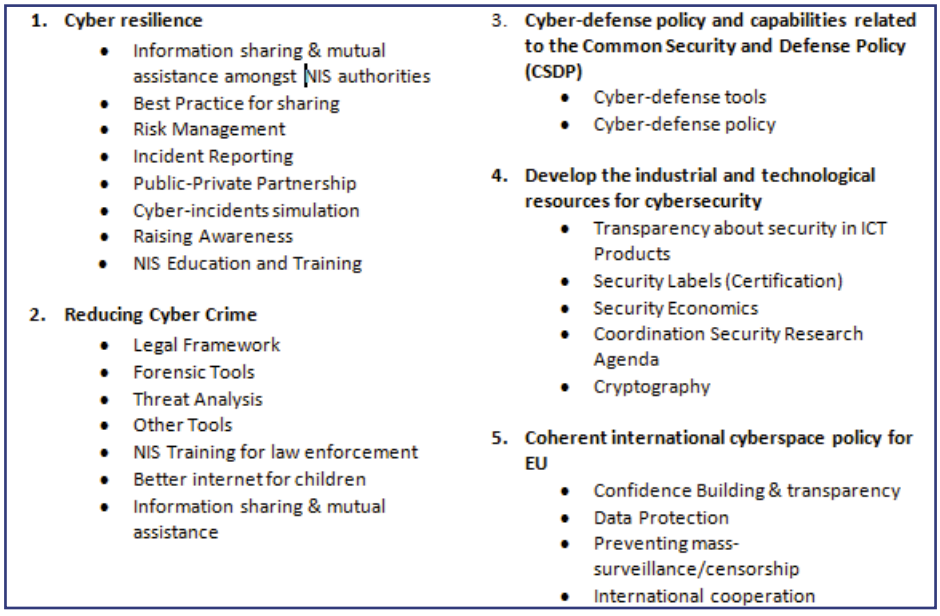

Fig. 1: The five Cybersecurity objectives extracted from EU cybersecurity strategies

8 http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security

2.1 Assessing Cyber Resilience

According to the EU Cybersecurity strategy, improving cyber resilience is related to the capability expressed both by public and private sectors to increase and enhance preparedness, cooperation, information exchange and awareness in the field of network and ICT Security. On this point the proposed NIS Directive suggests that concrete policy and regulatory measures will be developed and implemented in the national strategy of the Member States to maintain a minimum level of security and reliability in the network and information systems. Monitoring national competent authorities and newly formed computer emergency response teams (CERTs) will be responsible for handling risks and incidents.

Nevertheless, several ambiguities in defining and delineating member states cybersecurity roles, responsibilities and dependencies are possible. This issue has obviously a direct consequence to the proper implementation of Cybersecurity strategy and it generated a thorny and lively discussion about which businesses should be subject to the new NIS Directive rules. Even if there is full consensus on the need to target certain sectors (banking, health, transport and energy sector) given the "essentiality" of the services they provide[9], still the acceptance of the so-called "Internet Enablers", identified as a composite variety of entities working at different levels (e-commerce platform, Internet payment gateway, social networks, search engines, cloud computing services and application stores) is under debate.

The identification of the entities more vulnerable to cyber-attacks depends also on a long and complex procedure of risk assessment. A range of FP7 T&S projects target this issue working on the development and the improvement of new methodologies and tools for the risk evaluation.

Several efforts to assess cybersecurity on different levels (national, international, organizational)

The European Network and Information Security Agency through Deloitte performed a benchmarking activities include the CERT Operational Gaps and Overlaps study [ENISA, 2011] where the operational gaps and overlaps of national/governmental CERTs in Europe were analyzed and some recommendations were made.

A UNIDIR study [UNIDIR, 2013] in 2011 found that 68 of the 193 United Nations Member States had cybersecurity programs. Of those, 32 states included cyberwarfare in their military planning and organizations, while 36 states had civilian agencies charged with a domestic cybersecurity mission. In August 2012, the same assessment [UNIDIR, 2013] surveyed again publicly available information for the 193 states and found that the number of national cybersecurity programs had grown to 114. Forty-seven states have cybersecurity programs that give some role to the armed forces and 67 states have solely civilian programs.

The Economist Intelligence Unit and Booze Allen Hamilton has developed the Cyber Power Index over 19 countries of the Group of 20 [Economist Intelligence Unit and Booze Allen Hamilton, 2011]. This index is a dynamic quantitative and qualitative model, constructed using 39 indicators and sub-indicators, that measure specific attributes of the cyber environment across for drivers of cyber power: legal and regulatory framework, economic and social context, technology infrastructure and industry application.

The Global Cybersecurity Index (CGI) [ITU and ABI, 2015] is an ITU-ABI joint research project to rank the cybersecurity capabilities of nation states. The referential is based on five categories: Legal Measures; Technical Measures; Organizational Measures; Capacity Building; and Cooperation.

The Commonwealth Cybercrime Initiative (CCI) promotes a checklist used by CCI experts to do country assessment. The checklist includes elements such as the role of the national cybercrime strategy, securing nationalized ICT infrastructure, implementing a national search, review of legislation, a training resource needs analysis for law enforcement, etc.

There are also a large number of sector specific cybersecurity risk studies, such as:

- Reports elaborated by consulting firms that can be multi-sector (e.g. PWC [PWC, 2014]) or cross-country sector specific (e.g. Marsh Risk Assessment Research [Marsh & McLennan Companies, 2015]).
- National sectorial associations, for example the Electricity Subsector Cybersecurity Risk Management Process by the USA Department of Energy (DoE) [U.S. Department of Energy, 2012] that provides process for the electric sector, including the assessment of security posture and identification of gaps and needs.
- National centers for critical infrastructure protection In Switzerland, for example, MELANI

9 The ECI (European Critical Infrastructures) directive establishes a procedure for identifying and designating the European Critical Infrastructures and proposes a common approach for assessing the need to improve their protection.

This is the case of **PANOPTESEC** (Call 10) that will deliver a prototype for a cyber-defense decision support system supporting organizations in detecting the attacks and properly responding to them. This prototype will support further exploitation of the solution by critical infrastructure customers as well as transportation, banking, finance, government and defense markets, in line with the EU NIS Strategy and the National Strategies of the Member States. Risk prediction considering also non-technical issues is fostered by the Call 8 **TRESPASS** project, which aims at working on an attack navigator tool suite that assesses potential attack vectors and attack paths and provides to the defender an integrated risk assessment and decision support process for more efficient security investments. A user friendly technology to assess the risk is the major contribution of the project **MUSES** (Call 8), working on a user centric, device-independent and self-adaptive corporate security system that is able to analyze in real time the risk and trust for user actions performed with the device, that can be personal or owned by the company. **RASEN** (Call 8) contributed with innovations including a method for risk based security testing and legal compliance, and supporting open source tools (the CORAS tool set developed by SINTEF), which have been made available free for anyone to use.

2.2 Reducing Cybercrime

Threat analysis

At the infrastructure layer, anomaly detection and analysis in backbone Internet helps in understanding current threats and obtaining reliable knowledge. Several types of anomaly detectors with different theoretical background and application classifiers have been developed and several FP7 projects contributed in this field, like **NECOMA** (Call 10) and **SWEPT** (Call 10).

In addition, DNS query data are key data for threat analysis, while BGP trace analysis also highlights routing errors (e.g. the Pakistan/Youtube incident) or malicious activity such as yby spammers. Query data at root DNS servers or large cache resolvers can be analyzed for characterizing phishing activities with signal processing and machine learning techniques.

At the endpoint layer, the web server access logs and web traces can be analyzed in terms of threat detection and identification. These entries are direct evidence of threats, such as java script malware. **DEMONS** (Call 5) aimed at designing and demonstrating the operation of a network for cooperative monitoring: innovative measurement, analysis and data protection techniques have been applied across a network of flexible monitoring nodes in multiple domains to accomplish cooperation, resiliency, and scalability in measurement, and confidentiality of measured traffic.

Finally capacity building should cover analysis of the web users' behavioral data, although here data protection and privacy should be included as a part of educational accompanying service. The behavior analysis is interesting due to the increase of cyber-attacks targeted users in developing countries. This capacity could detect new aspects for identifying phishing attacks and executing untrusted programs.

Visual analytics

One common subject of the FP7 EU projects is the application of visual analytics or building customized analytic capability in threat areas specific for the group of trainees. Most of the analysis methods are based on sophisticated mathematical techniques such as, machine learning, signal processing, artificial intelligence, etc., but the courses may not enter into too much depth about specific methods. Many projects within FP7 work on visualization tools: **TRESPASS** (Call 8) developed a range of visualization techniques from formal models (e.g., attack trees) to physical models. 16 high-quality, exploitable software artefacts ranging from new data collection infrastructure to analytics modules and visualization components have been developed by the Call 5 project **VIS-SENSE**, together with a visual analytics framework, created with the goal of integrating these heterogeneous components into a single visual analytics system for network analytics.

Security requirements and notification

Mandating security requirements, as well as the obligation to report security incidents over a defined threshold to the designated authority, have raised a heated debate between EU bodies and EU stakeholders. One of the objections targets the security requirements implementation and points out that these new requirements should be compliant with security requirements already in place. More precisely, the question is how much overlap this

Directive could have with the notification rules that will be adopted in the forthcoming General Data Protection Regulation[10]. From the legislative point of view indeed, some EU stakeholders ask for a better design of the NIS: the European Central Bank warned EU legislators that imposing new security incident notification rules in the payments sector, creates conflicts with the reporting frameworks payment service providers are already subject to[11]. Moreover, reporting cyber security incidents might concern a breach of personal data which would need to be reported to data protection authorities, under the planned new General Data Protection Regulation.

Among the FP7 projects working on identification of security requirements we can list **POSECCO** and **ANIKETOS**, both from Call 5.

Contracts, agreements and certifications

Due to presence of multiple stakeholders interaction in present IT, agreeing on service level contracts, certification, and policies is becoming common. It is becoming critical to put in place controls to check that these agreements are actually enforced at runtime. Monitoring plays a major role and extensive research is devoted to put in place monitoring systems that constantly verify the enforcement, for example the above mentioned **CUMULUS** (Call 8) project is developing methods to check the validity of software certification and Call 8 **A4CLOUD** that has a similar approach for privacy policies. Also **AU2EU** project from Call 10 aims at working on policy enforcement mechanisms designing a joint eAuthentication and eAuthorisation framework for cross-domain and jurisdictional collaborations.

Enhancing the standardization process, the **CIRRUS** project (Call 8) aims at increasing the level of trust in Cloud computing, with the goals of supporting on-going research projects and coordinate a dialogue that will lead to a convergence of such efforts. CIRRUS delivered a Green Paper on Cloud Security and a CEN Workshop Agreement (CWA–RACS), who has received requirements and recommendations from other European projects such as **ASSERT-4SOA** (Call 5) and **PCAS** (Call 10). A confidential and compliant clouds is also the focus of **COCO CLOUD** (Call 8), delivering a data sharing agreement authoring tool, with legal and business compliance ensured by design (starting from the reutilization of the main outcome of the Call 1 **CONSEQUENCE** project) leveraging on predefined ontologies.

Data sharing and monitoring tools

One of the priority of NIS Directive lays in the data sharing and attacks notification process, directly handled by the Member States. Operators of critical infrastructure (energy, transport, banking, healthcare), key Internet enablers (e-commerce platforms, social networks, etc) and public administrations are requested to take appropriate technical and organizational measures to face the security risks related to networks and information systems, preventing and minimizing the impact of security incidents affecting the core services they provide. These subjects must also notify the competent authority of incidents having a significant impact on the continuity of these services. Nevertheless, this is matter of disagreement between the Commission's proposal and the Council: this last's position focuses mainly on the notification mechanism and considers the possible resistance to mandate the sharing of information[12].

Data sharing could be a problem in supply chain management, due to due to inherent risks associated with exposing private data. Aimed at building a trustable environment to share data and information, the ICT-PSP project **ACDC** (Call 8) developed a centralized platform for information sharing, called the "Clearing House" that intends to collect data from the stakeholders involved, process it and analyze it. A collaborative repository for cybersecurity data and threat information on top of a privacy-aware storage system (called TAMIAS) is designed by **NECOMA** (Call 10). Call 5 **SECURESCM** proposed to use secure computation to overcome problems in the data sharing process, enabling the secure collaboration and interoperation of supply chain partners to gain the advantages of knowledge-based collaborative supply chain planning, forecasting, benchmarking and management. Part of these outcomes have been implemented into the SAP's product HANA.

Also **PCAS** (CALL 10) developed a solution to ease the data sharing producing an innovative, trustworthy and handheld de-

10 http://www.out-law.com/en/articles/2015/march/uk-does-not-want-online-services-to-be-subject-to-new-cyber-security-rules-says-official

11 http://www.out-law.com/en/articles/2014/september/ecb-warns-about-conflicts-in-payment-system-security-incident-notification-requirements

12 http://www.scl.org/site.aspx?i=ed39127

vice: the Secured Personal Device (SPD), a smartphone accessory allowing users to securely store their data, to share it with trusted applications, and to easily and securely authenticate him, through biometric authentication mechanisms.

With the increasing complexity and dynamicity of software system, automated data collection based on monitoring tools is becoming a relevant topic for applied research. Two major trends are emerging: cross-stack data collection and contract/certification/policy enforcement.

In a nutshell, traditionally monitoring mostly focused on the network layer, recent re-search is addressing a more holistic approach, where information is collected and combined across the stack: network, platform and application level. Projects addressing multiple-levels include: **CUMULUS** (Call 8) which developed new tools for testing, monitoring and Trusted Computing proofs to support certifications, providing a novel infrastructure for certification of multi-layer cloud services; Call 5 **POSECCO** consolidated its prototype including the central model repository (the MoVE tool), a collaborative system for eliciting security requirements and high-level policy monitoring (the CoSeRMaS system), a tool for policy specification and conflict resolution (the IT Policy tool), a decision support system for security (SDSS), and tools for audit support and configuration validation.

Data Collection

A risk assessment always starts with data collection. The end objective is identifying and then implementing a corrective action plan that will improve data security in a cost-effective way, that is the right fit for the system analyzed. Therefore, the question in any risk assessment is how to move from the current state to a cost effective security.

The need to collect data on the cyber security events then requires to move in the direction of building a structured and rationalized set of records. Data collection can happen at several cyber space layers. Typically, the infrastructure layer encompasses both networks and hosting centers that together form the backbone and service side of the Internet, and the endpoint layer which encompasses all the terminals used to access the aforementioned infrastructure. Capacity building should cover many existing initiatives and solutions, to receive directly malicious attempts or observe background noise related to these malicious attempts (backscatter).

Some of the FP7 projects worked in this direction, providing solutions to gather data through the use of networks of honeypots and network telescopes. Call 10 **NECOMA** for example analyzes data both from an infrastructure perspective (networks and large computing infrastructures) and endpoints (smartphones and browsers). Infrastructure layer datasets include traffic, DNS, topology, telescope, and datasets from early warning systems; while endpoint layer datasets include mail and messaging, web, user behavior client honeypot and sandboxing. **NEMESYS** (Call 8) as well targets the identification of vulnerabilities in mobile devices and networks designing novel tools working as honeypots to attract and detect anomalies.

The enormous volume of information generated by these tools do not correspond to the little work in standardizing reporting and sharing which can link capacity building services to research analytics services. Still relatively little work has gone into capacity building related to extracting actionable knowledge from these collected data. In this field it is worth mentioning the successful exploitation of **MASSIF** (Call 5) outcomes: a real-time big data platform for Complex Event Processing run by the LeanXscale start-up.

2.3 Cooperation and collaboration

As mentioned before there are many benefits of sharing data and information. But which data, when, in what circumstances and what format? Capacity building could be structured around data targeting adversaries (attack indicators, techniques, targets, attacker's identities, etc.). Another angle is considering incidents and safeguards, including controls, security mechanisms and defensive techniques, etc. One of the most common cooperation and collaboration areas is related to vulnerabilities, where many standards exist. More specific and sensitive type of data is related to assets, employee observations, impact, business strategy, etc. Equally, events from SIEM (security event and information management tool), behavior data, control status, etc., are unlikely to be shared unless there is high trust such as among the governmental departments.

This is a very relevant topic for NIS platform. A number of EU and national projects are contributing with technology dealing with secure or privacy preserving information sharing and/or sharing of security data. **CYSPA** project (Call 8) for in-

stance, is one among few projects which worked on the development of an integrated EU strategy for protection of the cyberspace, setting up an European Cyber Security Protection Alliance to bring together EU stakeholders to articulate, embody and deliver the concrete actions needed to reduce cyber disruption. This would allow to respond more effectively to security incidents but also to remain informed of changes or evolutions in attack phenomena occurring in the monitored networks. With similar objectives, **DEMONS** (Call 5) aimed at designing the operation of a network for cooperative monitoring. This project significantly advanced the ability to detect and respond to large-scale threats. Several operational European Support Centers to raise awareness and provide support to stakeholders and end-users have been developed by **ACDC** project (Call 8). Moreover, ACDC promotes an integrated process among different stakeholders concerned with cyber security in Europe, and builds trusted relationships among them (crucial point to ensure a transparent and reliable data sharing).

From a technology perspective, current techniques under development rely on cryptographic methods (e.g., secure multi-party computation) and on data fragmentation and anonymization. **ASPIRE** and **PRACTICE** both funded under Call 10 rely on cryptography to introduce novel software-based protection mechanisms for mobile devices.

Trust among actors in cyber security

Trust is the key to allow citizen and business to consume the plethora of services of the internet. It can be declined at different levels, each of them has one or more trust building methods associated: consumer-facing applications may benefit by advanced reputation models and software certification (**OPTET**, Call 8), developers can build on trustworthy service development tools developed by projects like **ANIKETOS** (Call 5), system administrators and auditors can increase the trust on the software ecosystems by automatic verification of configuration (**POSECCO** from Call 5), software and network providers can increasingly rely on trustworthy hardware (**HINT** from Call 8).

Aspects of privacy

Finally, we can also add Privacy and data protection mechanisms as “trust building” mechanisms. These have been extensively investigated by research projects. Various approaches are present, targeting privacy-enhanced methods for authentication (**ABC4TRUST** in Call 5), designing of privacy-aware systems (**PRIPARE** from Call 10), or machine-readable privacy policy definition, negotiation and enforcement (**A4CLOUD** (Call 8), **COCOCLOUD** (Call 10) and Trust-in-the-Cloud EIT project).

Conclusion

The overview provided in this Whitepaper highlights a strong connection between the innovative results delivered and the topics researched by the FP7 projects and the priorities declared by EU policy intentions. The projects considered in this analysis address the EU Cybersecurity Strategy's objectives and are capable of providing expert contributions to the requests and recommendations expressed by the Strategy and the proposed NIS Directive.

In this document we presented the projects that have gained expertise and developed technologies in the domains we currently identified clustering the topics expressed in the EU Cybersecurity Strategy. Some considerations can be drawn on the general trends of the research outcomes compared to the to EU Strategic Cybersecurity priorities. The main areas addressed by the EU projects are:

- cyber resilience in terms of risk management, readiness, maturity, organizational measures for risk evaluation and integrated risk assessment;
- cybercrime reducing tools as threat analysis mechanisms, automated anomaly detection, data sharing and monitoring tools, data collection and security requirements;
- lastly, collaboration and cooperation among different actors through network for cooperative monitoring, support centers and data protection mechanisms for trust building.

In addition, as shown by this study, the panorama of research projects targeting ICT security in Europe is pretty vast and diverse and cover a wide array of topics and subtopics in the ICT T&S domain.

Looking at the next future, the H2020 Programme shows some difference in respect to the FP7 Programme that is about to finish. It tends to focus more for the first time on innovation and not on only research and development. This could mean a step closer to the deployment of the technologies and would consequently signifies a closer relationship with the industrial sector. The beneficial outcome of this contact could result in a more dynamic and effective European cyber environment, able to put together demand and supply.

References

- BIS, UK Department for Business, Innovation and Skills, 2014, "Information Security Breaches Survey 2014". Available online http://www.pwc.co.uk/assets/pdf/cyber-security-2014-technical-report.pdf
- Compagna L. and Bezzi M., 2014, SECCORD Deliverable 2.3. Year 2 Cluster Report. Available online
- De Gramatica M. and Massacci F., 2015, SECCORD Deliverable 3.3 – Annex 2 "FP7 ICT Trust & Security Projects Handbook"
- Economist Intelligence Unit and Booze Allen Hamilton, 2011. "*Economist Intelligence Unit and Booze Allen Hamilton Findings and Methodology*". Available online http://www.boozallen.com/media/file/Cyber_Power_Index_Findings_and_Methodology.pdf
- ENISA, 2011 "*CERT Operational Gaps and Overlaps*". Available online https://www.enisa.europa.eu/activities/cert/other-work/gaps-overlaps-report
- ITU and ABI, 2015, "*Global Cybersecurity Index & Cyber wellness Profiles*". Available online http://www.itu.int/dms_pub/itu-d/opb/str/D-STR-SECU-2015-PDF-E.pdf
- Marsh & McLennan Companies, 2015, "*Cyber Risk management: New Threats, New Approaches*". Available online https://www.marsh.com/content/dam/marsh/Documents/PDF/US-en/Marsh%20NROR%20Cyber%20September%202015.pdf
- MELANI, 2014, "*Information Assurance Situation in Switzerland and internationally*". Available online file:///C:/Users/martina/Downloads/MELANI_Semi_annual_report_2014_2.pdf
- PWC, 2014, "*Managing cyber risks in an interconnected world*". Available online http://www.dol.gov/ebsa/pdf/erisaadvisorycouncil2015security3.pdf
- UNIDIR, 2013, "*The Cyber Index. International Security Trends and Realities*". Available online http://www.unidir.org/files/publications/pdfs/cyber-index-2013-en-463.pdf
- U.S. Department of Energy, 2012, "*Electricity Subsector Cybersecurity Risk management process*". Available online http://energy.gov/sites/prod/files/Cybersecurity%20Risk%20Management%20Process%20Guideline%20-%20Final%20-%20May%202012.pdf

Appendix FP7 Trust &Security projects mentioned

PROJECT	CALL	CONTACTS
A4CLOUD	8	http://www.a4cloud.eu/
ABC4TRUST	5	https://abc4trust.eu/
ACDC	8	http://www.acdc-project.eu
ANIKETOS	5	http://www.aniketos.eu
ASPIRE	10	http://www.aspire-fp7.eu
ASSERT4SOA	5	http://www.assert4soa.eu
AU2EU	10	http://www.au2eu.eu/
CIRRUS	8	http://www.cirrus-project.eu
COCO CLOUD	8	http://www.coco-cloud.eu/
CUMULUS	8	http://www.cumulus-project.eu
CYSPA	8	http://cyspa.eu
DEMONS	5	http://fp7-demons.eu
HINT	8	http://www.hint-project.eu
MASSIF	5	http://www.massif-project.eu
MUSES	8	https://www.musesproject.eu/Muses
NECOMA	10	http://www.necoma-project.eu
NEMESYS	8	http://www.nemesys-project.eu/nemesys/
OPTET	8	www.optet.eu
PANOPTESEC	10	http://www.panoptesec.eu/
PCAS	10	http://www.pcas-project.eu/
POSECCO	5	http://www.posecco.eu/
PRACTICE	10	http://www.practice-project.eu/
PRIPARE	10	http://prepareproject.eu/
RASEN	8	http://www.rasen-project.eu
SECURESCM	5	http://www.securescm.org
SWEPT	10	http://www.swept.eu/
TRESPASS	8	http://www.trespass-project.eu
VIS-SENSE	5	http://www.vis-sense.eu

SECCORD / Security and Trust Coordination and Enhanced Collaboration

Contact Info

Prof. Fabio Massacci
Università degli Studi di Trento

seccord@unitn.it

www.seccord.eu