



UNIVERSITÀ DEGLI STUDI
DI TRENTO



YEARBOOK

FP7 ICT Trust & Security Projects Handbook

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

Foreword by Jakub Boratynski
Head of Unit - ICT Trust and Security

Afterword by Martin Mühleck
ICT Trust and Security - Programme Officer



FP7 ICT Trust & Security Projects Handbook
Version I, March 2015

© University of Trento

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.

The information and views set out in this publication do not necessarily reflect the official opinion of the European Commission or the projects described presented in the publication.

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.



All rights reserved.

This publication is distributed under the Creative Commons Attribution-NonCommercial-ShareAlike license CC BY-NC-SA, which means that you are free to copy and distribute this work under the following conditions:

Attribution - you must attribute the work in the manner specified by the author or licensor (but not in any way which would suggest that they endorse you or your use of the work).

Noncommercial - you may not use this work for commercial purposes.

Share Alike - if you alter, transform, or build upon this work, you may distribute the resulting work only under the same or similar license to this one.

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 A** 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/>

Foreword

The Digital Single Market is one of the European Commission's top priorities. It represents a golden opportunity: by fostering a Digital Single Market, the EU can create up to €250 billion in additional growth, hundreds of thousands of new jobs, and a vibrant knowledge-based society.

Trust and security in the digital world are the very foundations of a Digital Single Market. Millions of EU citizens rely on the Internet for ever more services, while at the same time this digital world is still vulnerable: technical failures and malicious attacks occur at alarming intervals and failure to respond to these incidents will mean consumers losing confidence in the digital world, businesses losing money, and even national security being put at stake.

European citizens have to know and trust that the systems underpinning the digital world are safe and secure, so they (and also business) can fully reap the benefits of the digital economy. The European Strategy on Cybersecurity launched in February 2013 sets out ways to strengthen network and information security across the EU to make Europe more trusted and secure online. In particular, the proposed Network and Information Security Directive – once adopted and implemented – will ensure a high common level of cybersecurity in the EU, by improving Member States' national cybersecurity capabilities as well as the cooperation between Member States, and also by requiring companies in critical sectors to adopt risk management practices and report major incidents to the national authorities.

Next to its legislative initiatives, the European Commission's priorities for a coherent Network and Information Security (NIS) across the EU include the direct support for research and innovation in those areas, where it can make a difference. The remaining projects funded by Framework Programme 7 (2007-2013) are now coming to an end, while the first projects under the new Programme

Horizon 2020 are currently being launched.

This is a perfect moment to look back at the entirety of FP7 to identify its successes and gaps and to draw conclusions for better addressing the cybersecurity challenges that lay ahead of us: What kind of projects worked out best to support society in Europe? What projects boosted the competitiveness of European industry by developing solutions and services? How can we best foster Europe's academic excellence in the field of trust and security? Some of these questions are currently answered by the NIS-Platform in an ongoing process, but in my opinion it is crucial to know your past, if you want to predict your future. The SECCORD project undertook the difficult task to collect and analyze the entirety of FP7 projects in the field of trust and security. They were able to distill from the available information a selection of success stories, while providing the full picture of past and ongoing research, which will lead to further examples of innovation and higher levels of protection.

The handbook provides a multitude of valuable insights and will serve us as a point of reference what EU-funded research and innovation can achieve and what inspiration can be taken from it for Horizon 2020. As you will see on the following pages, European scientists and companies are working hard to make the journey to a trustworthy digital world. I invite you to read these and join them in their effort so Europe can fully benefit from the opportunities in front of us. ■

Jakub Boratynski

Head of Unit of Trust and
Security,
DG CONNECT, European
Commission



Executive Summary

The FP7 Framework has funded several projects in ICT Trust and Security throughout the past 9 years and we showcase here the results of a comprehensive study and interviews of project coordinators, technical and scientific leaders.

For almost a decade, the FP7 Research and Development Framework Programme has funded research and development projects addressing the security and privacy of ICT (Information and Communication Technology) for a total of value of almost 361 million euro. A key question for policy makers and citizens alike is whether it was worth it: where are the European "success stories"?

This Handbook tries to address these questions through a comprehensive study of FP7 security and trust ICT projects in FP7. It is based on the analysis of public data and several interviews with project coordinators, technical and scientific leaders. The R&D projects which responded in May 2007 to Call 1 finished a few years ago and their results are making their inroad into the market. Call 5 Projects are reaching maturity, whereas Call 8 and Call 10 projects are still hammering their research results. Other projects from the Competitiveness and Innovation Framework Programme (CIP) have a shorter focus in their timing and are already delivering results to citizens and business. As a whole they have

delivered several innovative results which are summarized in this report.

From a technical perspective, all research projects funded by the EU Commission have undergone a review by competent experts, and have successfully presented their agreed technical deliverables. To a lay citizen this would hardly be a condition for being classified as "successful". What European citizens and policy makers want to know is how many research projects led to new companies, new jobs, new intellectual property, new international standards, and new experiences by ordinary citizens; how many projects have not (yet) achieved these goals but are at least going in the proper direction.

It is difficult to have a final judgement on such issues as the road of successful technologies is long and fraught with wrong turns and unexpected hurdles. Few digital natives would even imagine that the recording technology that allows us to enjoy music was considered by its first inventor, T. A. Edison in 1878, as a business's gizmo for "letter writing and all kinds of dictation". ■

What counts as a success story?

In order to decide what is a success story we should look at the overarching goal assigned by the European Union to DG Connect, and namely the "emergence of a European industry and market for secure ICT". From this perspective one can identify several concrete steps that European citizens would recognize as definite aspects of success story.

The first and foremost indicator is the creation of new jobs and companies:

- 1) the creation of a spin-off company to finalize and commercialize the results of a project (e.g. the spin-off Partisia after the CACE project results or the VC investments in the startup Key-Lemon after TABULA RASA);
- 2) the internal follow-up with new human resources assigned by a company to the further development and commercialization of a product's outcome in a product (e.g. SAP follow-up of the technologies from SECURESCM);
- 3) the incorporation in whole or in part of the actual

technology in a product or a production process (eg SAP incorporation of SPACIOS technology into its development toolkit);

- 4) the creation of valuable intellectual property worth patent protection (e.g. the three patents out of CONSEQUENCE's result).

A different, but equally valuable direction, is the general contribution to a more secure digital ecosystem. In this realm we can include

- 5) the adoption by other companies and citizens of the specific research results leading to a safer internet (e.g. Google, which never participated to EU R&D projects, acknowledged that AVANTSSAR technology contributed to secure Google's own services);
- 6) the contribution to world-wide standards on secure and privacy-preserving technologies (e.g. ABC4Trust ISO/IEC standardization);
- 7) the distribution of project results as open source components and their take up by the community at large.

On the road to the successful deployment into the market that we have described above, research project must be ready to go outside university and industry laboratories. From this perspective we can also classify as success stories projects that

8) piloted their technologies with citizens and end users (e.g. ABC4Trust piloting its technology in a Swedish school or PICOS experimenting with anglers) or

9) made their services available on the web for everybody to use (eg ACDC availability of a web service for checking malware on the web).

Not all research projects are at the same state of development and this must be necessarily reflected in the assessment and how far they have fulfilled at least one of the above criteria. Some projects have been funded at the beginning of the FP7 Framework programme and have already ended by several years; the projects funded at Call 10 have not yet finished and only few of them could obviously provide evidence for success stories.

The handbook showcases success stories of 12 European projects in ICT Trust and Security according to the above mentioned criteria. The selected projects have been funded with 49 million euros, 14% of the total EU budget spent in FP7 ICT security and trust projects of around 361 million euros¹.

The remaining projects have been clustered in the following sections, according to their achievements towards their potential innovation in the EU security market and their willingness to discuss and share their results.

- The section on **"Innovative Projects working towards the market"** focuses on the recent developments achieved by projects from Call 10, 8, 5

and 1. They are reaching maturity, validating their results through different means (pilots, testbeds, experiments) and approaching to the market arena, occasionally bumping into challenging gaps. They have shown us some evidence that at some point they might become success stories. These 19 projects have been funded for € 80 million euro, namely 22% of the total EU budget spent in FP7 ICT projects in security and trust

- We grouped into the **technical successful Projects** section the 18 projects who had been interviewed in the past and did not update their status in this last round. These projects present their objectives and how they are planning to produce innovation for the market but did not provide evidence that they could actually become success stories at some point; the total amount of contribution allocated is almost 85 million euro (23%).

- **Community building activities** (Coordination and Support Actions and Network of Excellence projects) are clustered in a separate section as they aim at providing effective, practical and useful means of communications, coordination, networking and dissemination, through use of knowledge studies or expert groups assisting the implementation of the Framework Program. Under these funding schemes 17 projects have been funded, for a little less than 23 million euro - 6% of the total.

- The last section ends with a short description of the 32 projects which did not reply to our requests of sharing and discussing the innovation potential of their technical results. These **other R&D projects** have been funded for € 124million euro (34%). They mostly belong to Call 1 and 5. ■

Does European research programme in ICT security and trust deliver value for money?

The European Commission funding of 361 million euro pales against the investment of venture capital in ICT security: according to data collected by Thomson Reuters², venture investors put nearly 3 billion of US dollars into cyber security companies between 2011 and 2013, resulting in new funding for some 300 firms.

According to Forbes research³, only one in 10,000 funded start-ups end up being worth over 1 billion of US dollars. In terms of "normal" outcome, only one in 10 portfolio companies is a big winner; about three of them may return the investment; and the rest go out of business. The jury is still out on the European research project leading to a 1 billion euro in return, but for normal, market-level return on investment the success

rate of at least 13% of EU funded project is essentially the same of a venture capitalist. For an administration that is often accused by its citizens of being mired in bureaucracy, claiming the same success rate is far from being a bad result. One question that may intrigue European policy makers is whether there is a "golden rule" for what makes a successful project. In this study, it was not possible to identify one rule which would work beyond doubt. Some large projects yielded noticeable results, albeit after continuous funding to essentially the same consortium across multiple calls. Lean and medium projects may be the ones which deliver the best value for money: having a clear focus and tight collaborations seems the most effective way to be successful. ■

¹ We estimated these EU Contributions on the basis of Cordis information (http://cordis.europa.eu/projects/home_en.html)

² <http://www.darkreading.com/venture-capital-the-lifblood-behind-security-innovation/d/d-id/1234834>

³ <http://www.forbes.com/sites/petercohan/2014/01/03/will-venture-capital-beat-the-market-in-2014/>



**Martina
de Gramatica**



**Fabio
Massacci**

TABLE OF CONTENTS

Foreword	3
Executive Summary	5
1 Success Stories	9
• ABC4TRUST.....	10
• ACDC.....	13
• AVANTSSAR.....	14
• CACE.....	15
• CONSEQUENCE.....	16
• HINT.....	17
• PICOS.....	19
• SECURED.....	20
• SECURESCM.....	22
• SPACIOS.....	23
• TABULA RASA.....	25
• WSAN4CIP.....	27
2 Innovative Projects working towards the market	29
• ASPIRE.....	30
• AU2EU.....	32
• COCO CLOUD.....	34
• ENVIROFI.....	36
• INTER-TRUST.....	38
• MASSIF.....	39
• MUSES.....	42
• NECOMA.....	43
• NEMESYS.....	45
• OPTET.....	46
• PCAS.....	47
• POSECCO.....	50
• PRACTICE.....	52
• RASEN.....	53
• SWEPT.....	54
• TRESCCA.....	56
• TRESPASS.....	58
• UTRUSTIT.....	59
• VIS-SENSE.....	61
3 Technical projects	63
• A4CLOUD.....	64
• ANIKETOS.....	65
• ASSERT4SOA.....	66
• COMIFIN.....	68
• CUMULUS.....	69
• D-MILS.....	71
• EURO-MILS.....	72
• FutureID.....	73
• GENOM.....	74
• MASTER.....	76
• MATTHEW.....	77
• MICIE.....	78
• PANOPTESec.....	79
• SPECS.....	80
• STANCE.....	82
• TAMPRES.....	84
• UAN.....	85
• VIKING.....	86
4 Community Building Activities Projects	89
5 Other R&D Projects	97
Conclusions and Afterword	103

1

SUCCESS STORIES



Achieving trust with minimal disclosure

ABC4TRUST

Attribute-Based Credentials for Trust

Coordinator

Coord. Johann Wolfgang Goethe University
Frankfurt (DE)

Partners

Technische Universität Darmstadt (DE)
Alexandra Institute AS (DK)
Unabhängiges Landeszentrum für Datenschutz (DE)
Computer Technology Institute & Press -
Diophantus (GR)
Eurodocs AB (SE)
IBM Research - Zurich (CH)
CryptoExperts SAS (FR)
Miracle A/S (DK)
Microsoft Belgium NV (BE)
Nokia Networks (DE)
Söderhamn Kommun (SE)

ABC4Trust

Call  4 Years
(2010-11-01 to 2015-02-28)



10 Partners



7 Countries



€ 8.849.998 EU Contribution



<https://abc4trust.eu/>

«One of the possible innovations resulting from this project is to introduce new e-Identity concepts and new e-Identity management techniques. The focus is on the user.

This is the new element: it is up to the user to uncover the elements of his identity that he really wants to release to the service, or to uncover only the parts of his identity needed for the service.

So the innovation will be mainly the empowerment of the user, so that his e-Identity is in his han». **Yannis Stamatou**
(Diophantus - Computer Technology Institute & Press)

Privacy-ABCs provide both security and trust in the verified information for relying parties, and at the same time preserve privacy for the users by enabling pseudonymous or even anonymous authentication. They allow to securely verify individual attributes out of a certificate and proofs over selected attributes.

This means, **users can disclose only the information necessary for a specific transaction instead of sending a complete set of identifying data. Privacy-ABCs have the potential to replace common signatures and PKIs.**

This would be a big step towards empowering of the users, who regain control over their personal data.

In general, Privacy-ABCs provided the following benefits:

- **The concept of "partial identities"** helps to maintain different spheres of life: Due to the unlinkability feature of Privacy-ABCs, different accesses to a service portal by the same user do not have to be linkable. This means, for instance in case of the school communication platform, that a pupil's activities in a discussion are not linkable to his request for advice the other day, when he was troubled by a taboo problem.
- **Privacy-ABCs support the legal principle of data minimisation:** Due to the selective disclosure of attributes feature, the user can partition and recombine the credentials in a self-determined way. She is enabled to reveal only the attributes absolutely necessary to make use of a specific online service instead of always giving away the whole set of identifying data as stored, for instance, on her national eID.

At the same time, this means that people are in control over their own data: They know exactly which information they disclosed to whom.

- **Verifiers can rely on assured and focused information.**

Furthermore, ABC4Trust achieved:

- **Predicates/computations over attributes:** The user does not have to reveal her exact birth date but can just provide prove that she is of a certain age.
- **Use of attributes from different credentials – of different issuers – to create one token:** The user is enabled to combine the attributes she needs to provide proof of from different credentials. This leads to flexibility.
- **"Partial identifiers" based on pseudonyms:** The user might want to be linkable, e.g. when following an ongoing discussion in a chat room over several days. This "user-controlled linkability" is possible by reusing a self-chosen alias when logging in to the chat room again the next day.

A short and entertaining introduction to Privacy-ABCs is available as video clip on the ABC4Trust website¹.

⁵ <https://abc4trust.eu/index.php/press/2011-11-08-14-42-18>

INNOVATION ACHIEVEMENTS

ABC4Trust's results are the successful deployment of Privacy-ABCs in practice (pilot trials), the development of a common unified architecture for federating and interchanging different Privacy-ABC systems (Idemix by IBM and U-Prove by Microsoft), a framework for comparing them and a reference implementation (available publicly on GitHub²) of the components defining an ABC system.

Furthermore, ABC4Trust has moved Privacy-ABC technology to mobile platforms (smartphones and tablets).

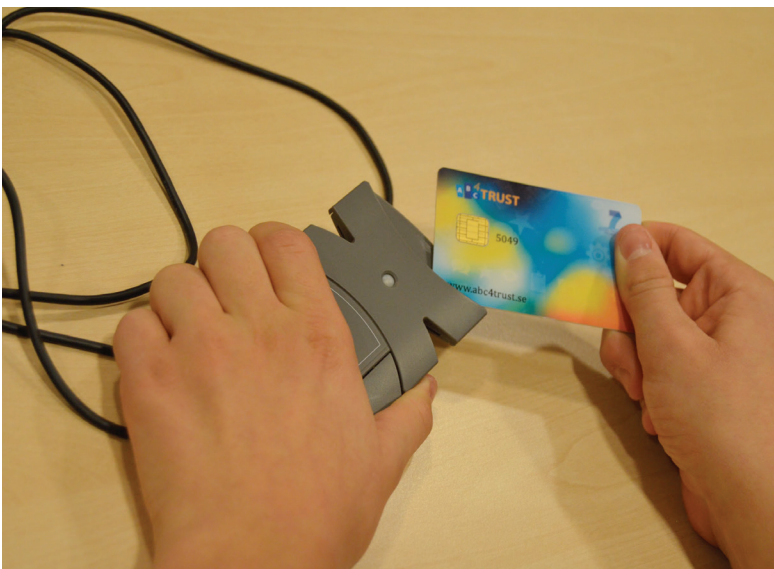
Another important factor for the usage of Privacy-ABCs is standardization. ABC4Trust is participating in ISO/IEC standardization (in ISO/IEC JTC 1/SC 27/WG 5 "Identity management and privacy technologies") and has contributed to a number of standards including ISO/IEC 24760-1: "A framework for identity management - Part 1: Terminology and concepts" and ISO/IEC 29101 "Privacy architecture framework".

MARKET INVOLVEMENT

ABC4Trust presented its research results at several conferences including the well-attended ABC4Trust Summit event³. Several consortium members of ABC4Trust are planning to launch Privacy-ABC technology in the near future. Furthermore, ABC4Trust published a book summarizing all project achievements which serves as a multiplier of the lessons learned from the project. It is available online and as print version⁴.

PILOTS

ABC4Trust set up a **privacy-preserving communication network in Norrtullskolan School in Söderhamn, Sweden**. Compared to other social networks, the ABC4Trust communication network does not allow to link cross context, if the same user name is employed in different settings. **The pupils, their teachers, and their guardians were enabled to exchange information securely by acting pseudonymously or even anonymously**. Based on the results of an anonymous questionnaire that was circulated after the trial it can be said that the target group understood the objective of the project and the concept of Privacy-ABCs. Moreover a large majority of the target group also stated clearly that there is a high interest in being informed about which personal data they reveal and how they can control it.



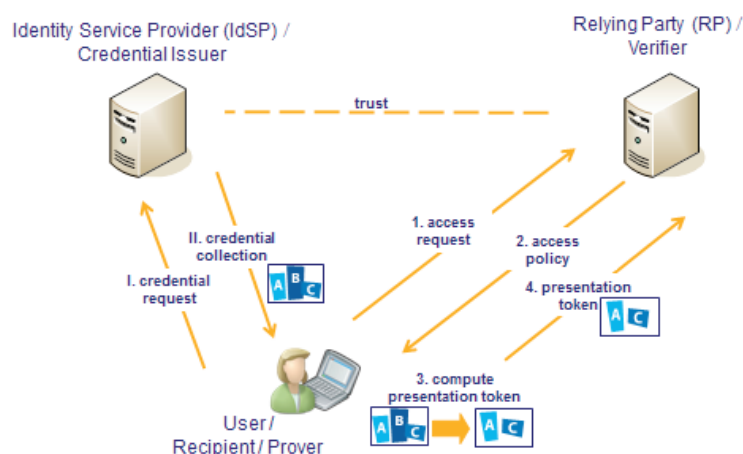
² <https://github.com/p2abcengine/>

³ <https://abc4trust.eu/index.php/events/177-summit-announce>

⁴ <http://link.springer.com/book/10.1007/978-3-319-14439-9>

ABC4Trust also implemented a course evaluation system at Patras University, Greek. The students were enabled to evaluate their courses anonymously, while the system guaranteed that only duly accredited students could participate in the evaluation. The technology acceptance among the students was good. According to the results of an anonymous questionnaire, they trusted the system and were convinced that their privacy was preserved. The majority of the students supported the idea of employing Privacy-ABCs also in other online services such as social media, blogs and e-shopping.

"The respective authorities are happy with the pilots and the feedback and there is a lot of interest in the ABC4Trust results. So in the not so far future one can expect more European public services and other organisations to switch to Privacy-ABCs", said the Coordinator of the project. Prof. Dr. Kai Rannenberg, Goethe University Frankfurt.



ABC4Trust architecture and process flows



ABC4Trust at the "EU Cybersecurity Strategy - High Level Conference" in Brussels, February, 28th, 2014. Keynote Speaker Dr. Thomas Kremer, Member of Deutsche Telekom's Board of Management for Data Privacy, Legal Affairs and Compliance, showing great interest in the ABC4Trust pilot and trial systems

An European anti-botnet pilot action



ACDC

Advanced Cyber Defense Centre

ACDC project is an European anti-botnet pilot action. It is a ICT-PSP project that includes 28 partners in 14 member states. Partners include IT security companies, ICT companies not specifically focused on security, ISPs, CERTs, government institutions, associations, research institutes.

The main objective of ACDC is to **detect and mitigate botnets from operating in Europe**. The project does this by integrating and deploying technologies to detect botnets (these include network security sensors deployment, and tools for collecting and processing the sensor data).

INNOVATION ACHIEVEMENTS

The main achievements of ACDC can be summarized as:

- a **centralized platform for information sharing called the Clearing House** that intends to collect data from the stakeholders involved, process it and analyze it;
- **several operational European Support Centers** to raise awareness and provide support to stakeholders and end-users. Moreover it promotes an integrated process among different stakeholders concerned with cyber security in Europe, and builds trusted relationships among them.

OVERCOMING CONSTRAINTS OF THE MARKET

The success of ACDC relies on its ability to receive the necessary data from the network sensors installed by ISPs in Europe, and to process these data. Therefore the main constraint to successful exploitation of the project is the legal framework enabling the project to access these data, which currently is very fragmented in Europe.

The project includes legal experts that work on identifying the best practices for ACDC collaborations with ISPs and other stakeholders that are compliant with the European regulations. ACDC will also prepare a report for policy makers about the legal challenges the project has faced and what aspects of the European data privacy laws could be addressed to facilitate fighting botnets.

MARKET INVOLVEMENT

The project has already created an infrastructure to detect and fight botnets (the Clearing House), and to assist citizens and organizations in improving security of their computers; in this sense the main provisioning for these potential customers is through the support centers. After the end of the project, ACDC will evolve into the European center for advanced cyber-defense.

PILOTS

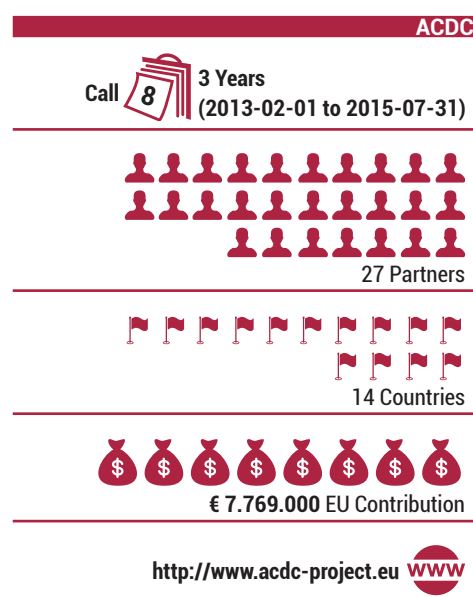
Actually, ACDC is a validation project in itself as its aim is to integrate different technologies that have already set to be released, and as such it includes many activities for validation and exploitation of the project technologies and tools. These activities include experiments on real infrastructures in European countries like Italy here Telecom Italia is involved, Belgium with LSEC participation and Croatia through CARNet Service contribution; and also public cyber security services for citizens.

Coordinator

Coord. ECO - Association of the German Internet Industry (DE)

Partners

ATOS (ES), Barcelona Digital (ES), Bulgarian Posts (BG), Cassidian Cybersecurity (FR), Cognitive Security (CZ), CARNet (HR), CyberDefcon (UK), DFN-CERT (DE), DE-CIX (DE), Telecom Italia (IT), ENGINEERING (IT), FCCN (PT), FKIE of Fraunhofer (DE), G Data Software (DE), Institute for Internet Security (DE), Inteco (ES), ISCOM (IT), Catholic University of Leuven (BE), LSEC (BE), Microsoft EMEA (FR), Montimage (FR), CERT-RO (RO), SignalSpam (FR), TECHNIKON (AT), Telefonica I&D (ES), Technical University of Delft (NL), XLAB (SI), Institute for Internet Security (DE)





AVANTSSAR

Automated VALidationN of Trust and Security of Service-oriented ARchitectures


Coordinator

University of Verona (IT)

Partners

ETH (CH),
INRIA Nancy (FR),
IRI Toulouse (FR),
University of Genoa (IT),
IBM Research Lab (CH),
OPENTRUST (FR),
Institute e-Austria Timisoara (RO),
SAP (DE),
Siemens (DE)

ABC4Trust

Call  3 Years
(2008-01-01 to 2010-12-31)


10 Partners


6 Countries


€ 3.800.000 EU Contribution

 <http://www.avantssar.eu>

OBJECTIVES

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

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

INNOVATION TARGETS

The project has developed:

- ASLan++ - a formal language for specifying trust and security properties of services, their associated policies, and their composition into service architectures.
- Automated techniques to reason about dynamic composite services, and their associated security policies.
- The AVANTSSAR validation platform - an automated toolset for validating trust and security aspects of service-oriented architectures.
- A library of validated composed services and service architectures, proving that our technology scales to envisaged applications.

IMPACT

Migrating project results to industrial development environments and standardization organizations may speed up the development of new network and service infrastructures, enhance their security and robustness, and increase the public acceptance of emerging IT systems and applications based on them. The project has included the WP6 Industry Migration to facilitate exploitation of the AVANTSSAR results; experiences and lessons learned during the AVANTSSAR technology migration are presented in the deliverables of this work package.

NEXT STEPS

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

HAVE A LOOK AT

The AVANTSSAR platform is accessible at the project website, including a comprehensive user manual.

A report on the platform was presented in the paper "The AVANTSSAR Platform for the Automated Validation of Trust and Security of Service-Oriented Architectures" by A. Armando et al. presented at the 18th International Conference on Tools and Algorithms for the Construction and Analysis of Systems (TACAS'2012)



CACE

Computer Aided Cryptography Engineering

The project had the ambitious objective of developing a toolbox to support high quality cryptographic software design.

Development of hardware devices and software products is facilitated by a design flow, and a set of tools (e.g., compilers and debuggers), which automate tasks normally performed by experienced, highly skilled developers. However, in both hardware and software examples the tools are generic since they seldom provide specific support for a particular domain. The goal of this project is to design, develop and deploy a toolbox that will support the specific domain of cryptographic software engineering. Ordinarily, development of cryptographic software is a huge challenge: security and trust is mission critical and modern applications processing sensitive data typically require the deployment of sophisticated cryptographic techniques.

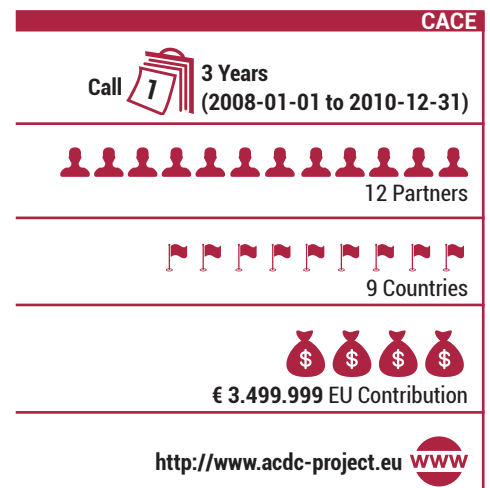
The proposed toolbox will allow non-experts to develop high-level cryptographic applications and business models by means of cryptography-aware high-level programming languages and compilers. The description of such applications in this way will allow automatic analysis and transformation of cryptographic software to detect security critical implementation failures, e.g., software and hardware based side-channel attacks, when realizing low level cryptographic primitives and protocols. Ultimately, the end result will be better quality, more robust software at much lower cost; this provides both a clear economic benefit to the European industry in the short term, and positions it better in dealing with any future roadblocks to ICT development in the longer term.

MARKET INVOLVEMENT

CACE project developed two successful start-ups bringing their solutions to the market: Partisia (a spin-off of Aarhus University) offers secure auction-as-a-service, and Dyadic Security (a spin-off of Bristol and Bar Ilan Universities) markets a technology to store cryptographic keys in a distributed way. Nokia, another partner in the project, now deploys an advanced cryptographic mechanism in its phones.

Coordinator
TECHNIKON (AT)

Partners
Aarhus Univesitet (DK)
Alexandra Instituttet a/s (DK)
Berner Fachhochschule (CH)
Nokia OYJ (FI)
Ruhr-Universitaet Bochum (DE)
Sirrix Aktiengesellschaft (DE)
Technische Universiteit Eindhoven (NL)
Teknillinen Korkeakoulu (FI)
Universidade Do Minho (PT)
University of Bristol (UK)
University of Haifa (IL)





CONSEQUENCE

Context Aware Data-centric Information Sharing

Coordinator

Europäisches Microsoft Innovations Center GMBH (DE)

Partners

Hewlett Packard Italiana (IT)

Imperial College of Science, Technology and Medicine (UK)


The Science and Technology Facilities Council (UK)

Consiglio Nazionale delle Ricerche (IT)

Create-Net (IT)

BAE System LTD (UK)

CONSEQUENCE

Call  3 Years
(2008-01-01 to 2010-12-31)


7 Partners


3 Countries


€ 2.899.895 EU Contribution

 <http://www.consequence-project.eu/>

Today's society strongly relies on trustworthy, efficient and fast data exchange in different fields of the daily life. But such data exchange should respect the confidentiality or privacy of the data. Nevertheless, the concerns raised by these issues do not always match with the current security measures available and applied. Therefore the need to deliver a technology that could effectively provide a solution for these more and more challenging issues.

CONSEQUENCE project delivers an **architecture within a framework to enable dynamic management policies; these architecture is based on agreements ensuring end-to-end secure protection of data-centric information.**

INNOVATION ACHIEVEMENTS

The project developed a **Data Sharing Agreement Authoring Tool** to support company in finding the mechanisms that is right for them. This tool allows to formally express data sharing agreements in a special language CNL4DSA, supporting policies for data access authorization, obligation and prohibition. The result has been achieved combining several drafting data policies in agreements; analysis and consistency checking of agreements; policy based control of data access and of information rights management at use.

MARKET INVOLVEMENT

This result went from a scientific paper to a world-wide patent. Indeed **the technology has been patented by Hewlett-Packard Development Company**, a partner in CONSEQUENCE.

PILOTS

The results of CONSEQUENCE have been validated from a technical and business point of view via two test beds on the sensitive scientific data and the crisis management data. The first one was led by the Science and Technology Facilities Council and aimed at evaluating the flexibility of the framework in reference to variations in data volumes and in sharing policies; the testbed also wanted to assess the efficiency of enforcing the required security, without imposing unnecessary constraints and delays. The second one was run by BAE Systems partner and dealt with the management of sensitive data in case of emergency situations in civil and military cases.



HINT

Holistic Approaches for Integrity of ICT-Systems

«The HINT project is the first EU project looking at the issue of authenticating an Integrated Circuit and checking its integrity to tackle issues like counterfeiting or hardware corruption. The overall approach is to say that if I am to find out about the level of trust I can have in the chip, I can try to first authenticate the chip, using biometric signature like technologies (PUF), and then once I have authenticated the chip I can check that there is no malicious circuit within it». **Jacques Fournier, project coordinator**

OBJECTIVES

The HINT project works on holistic approaches for **enhancing trust in hardware devices based on two main technologies: Physically Unclonable Functions (PUFs) that allow chip authentication, and side channel analysis-based Hardware Trojan (HT) detection approaches** that allow chip integrity verification and counterfeit detection. A particular focus of the project is the future industrial exploitation of developed technologies, as currently existing approaches based on PUFs and HT detection schemes are not suitable for mass deployment due to the lack of stability with respect to changing environmental conditions.

RECENT DEVELOPMENTS

HINT has designed a novel PUF technology for chip authentication. This new technology, which is currently being fabricated, offers unprecedentedly strong stability with respect to external conditions, making it fully suited for industrial products. In order to cover the complex issue of Hardware Trojan (HT) detection, the project has studied several measurement (power, EM, timing information...) and detection (passive, active, passive, on-chip, off-chip) alternatives. Each one of them has been implemented and demonstrated. Their robustness and limitations are currently being studied.

Finally, in order to illustrate **the use of those technologies in real-life products, two demonstrators are currently being implemented: PUF-based signature key protection in an ID card** (led by Morpho company); **and HT detection in a Professional Mobile Radio (PMR) terminal** (led by one of our partners, Cassidian Cybersecurity, a major manufacturer of PMRs in Europe).

VALIDATION STRATEGY

The project works on two main case studies: unclonable ID cards and Professional Mobile Radio (PMR) communications. HINT plans three demonstrators. The first one is an industry-oriented HT detection demonstrator based on the platform used in PMR terminals.

The second demonstrator will be a practical smart card-based scenario where an embedded PUF structure is used for providing digital signature.

Finally, in order to show-case how the two researched technologies can work together to assure integrity in the sense of a holistic approach, a third demonstrator has been defined by the consortium, which will be implemented during the last project year. This last (laboratory) demonstrator will show how both technologies can be integrated together to enforce hardware trust: by doing so, the HINT project is going beyond the initial project's objectives.

Coordinator

TECHNIKON (AT)

Partners

Infineon Technologies Austria AG (Austria)

Catholic University of Leuven (Belgium)

CEA-LETI (France)

ARMINES (France)

Cassidian Cybersecurity (France)

Morpho Cards (Germany)

HINT

Call  **3 Years**
(2012-10-01 to 2015-09-30)


7 Partners


9 Countries

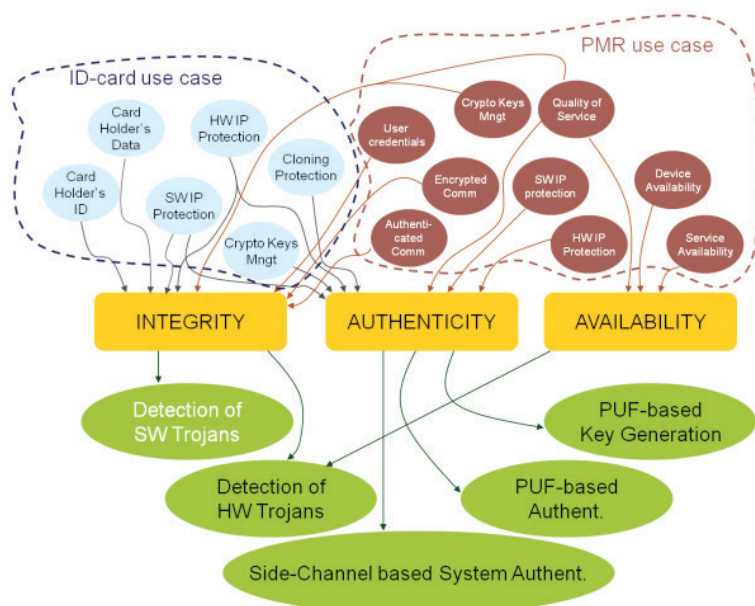

€ 3.350.000 EU Contribution

<http://www.hint-project.eu> 



IMPACT

Two patents have been filed so far by two of the project partners. The research works done in HINT have been presented at high profile international conferences like CT-RSA2014, DATE2014 and Chip-To-Cloud2014. The partners of the HINT consortium are also currently laying the foundations for a new ISO standard for the PUF technology.



Summary of HINT requirements



PICOS

Privacy and identity management for community services

OBJECTIVES

The main goal of the PICOS project was to advance the state-of-the-art in technologies providing privacy-enhanced identity and trust management features within complex services such as online communities managed by mobile communication service providers.

PICOS aimed at building and trying out with real users of a privacy-respecting identity management platform that supports provision of online community services and a client application for this platform.

INNOVATION ACHIEVEMENTS

PICOS has delivered the following innovative technologies:

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

IMPACT ON REGULATION AND MARKETS

The PICOS results can support developments in the EU policy and regulations for privacy protection and protection of minors on the Internet. **The project has run pilots with real end-users from an online gaming community and an angler community and has gained a lot of insights of the society requirements on privacy.** Results of the pilots show the applicability of privacy-enhancing concepts for mobile communities that are compliant with the upcoming General Data Protection Regulation.

In two cycles of trials **PICOS developed and improved concepts that resulted in innovative products and systems by several of the involved partners, especially Atos, HP, and IT-Objects.** The latter partner also ported the concepts from Symbian to Android for a higher sustainability.

Coordinator

Goethe University Frankfurt (DE)

Partners

HP (FR, UK)

Deutsche Telekom (DE)

Atos Origin (ES)

University of Malaga (ES)

CURE (A)

Catholic University of Leuven (BE)

IT-Objects (DE)

Leibniz Institute of Marine Sciences (DE)

Masaryk University in Brno (CZ)

PICOS

Call  3,5 Years
(2008-02-01 to 2011-06-30)

 10 Partners

 7 Countries

 € 3.999.998 EU Contribution

<http://www.picos-project.eu> 

HAVE A LOOK AT

Have a look at the demonstration videos of some of the project's results at the website www.picos-project.eu/Concepts-Features.204.0.html



SECURity at
the network **ED**ge

**A unique security
for multiple devices**

SECURED

SECURity at the network EDge

Coordinator

Politecnico di Torino (IT)

Partners

Hewlett-Packard (UK)

PrimeTel (CY)


Universitat Politècnica de Catalunya (ES)

Telefonica Investigacion y Desarrollo SA (ES)

United Nations Interregional Crime and Justice
Research Institute (IT)

VTT Technical Research Centre of Finland Ltd (FI)

SECURED

Call  3 Years
(01.10.2013 to 30.09.2016)


7 Partners


5 Countries


€ 2.700.000 EU Contribution

 <https://www.secured-fp7.eu/>

«Currently the protection of end-user devices is not uniform. If you have a laptop – you have plenty of software that can be installed. If you have a smartphone – a bit less, for security. If you have an in-car entertainment system connected to the Internet – you have none. The smart TV or smart fridge are the same. So it was an unsatisfactory offer of protection for end-user devices that drove us to proposing this solution». **Antonio Lioy**

The users own many Internet-connected devices today, but these do not offer uniform protection because of the proliferation of their form-factors and capabilities.

Thus the users need to take care of protecting each of these devices independently, and often the protection measures available are insufficient (for example, smart TVs do not have firewalls) or the users are not able to configure the devices correctly.

The SECURED project aims to protect users from network threats by **moving the security from the end-user devices into a suitable place inside the network** (e.g. a home gateway or a WiFi access-point), **empowering the user with the ability to define once the desired protection for all her devices and have it applied automatically at the point where she connects to the network**.

The project aims at facing the lack of uniformity in the protection of the end-user devices as stated by the coordinator.

INNOVATION ACHIEVEMENTS

SECURED works on:

- the architecture of a **programmable device to host the security applications off-loaded from the end-user terminal** (it will be possible to implement this device in hardware or as a virtual device running purely as software);
- a set of protocols to interact with and an implementation of this programmable device as a virtual device built on top of open-source components;
- a mechanism to simplify definition and application of the user's security policies for the applications run at the SECURED device.

OVERCOMING CONSTRAINTS OF THE MARKET

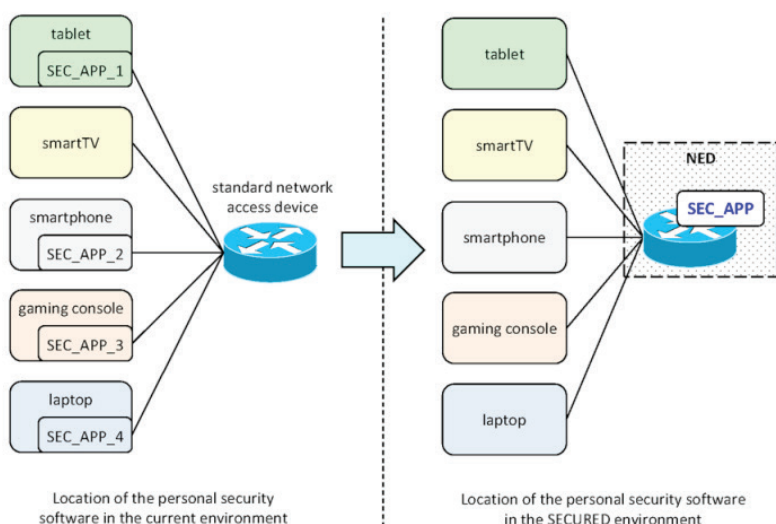
The SECURED consortium expects that the market is ready for its products. Potential challenges to the successful exploitation for SECURED might be the user awareness and conflicts with other existing security components.

MARKET INVOLVEMENT

The security device designed by SECURED will allow the users (as well as system administrators in an enterprise environment) to configure the security of many consumer devices with specific policies in an easier and more user-friendly manner.

At least two commercial partners are planning to exploit the results: **HP is interested in offering these network devices and Telefonica is exploring the use of this architecture to provide a better service to its customers.**

Moving security applications from user terminals to the network (Network Edge Device, NED)



PILOT

The project will run two pilots.

One pilot will focus on the **home gateway scenario**: it will be managed by the SECURED partner PrimeTel and will involve its actual subscribers (real end-users).

Another pilot will be focused on the **corporate security scenario** and will be run by VTT.




SECURESCM

SECURE Supply Chain Management

Coordinator
SAP (DE)

Partners
University of Milan (IT)
University of Mannheim (DE)
Technical University of Eindhoven (NL)
Zaragoza Logistics Center (ES)
Dhitech Technological District in Puglia (IT)
International University European Business School (DE)

SECURESCM

Call  3 Years
(2008-02-01 to 2011-01-31)


7 Partners


4 Countries


€ 2.099.996 EU Contribution

 <http://www.securescm.org>

OBJECTIVES

It is a well-known fact that **collaborative supply chain management and planning reduces production overall costs**. Nevertheless it is not being exploited due the fact that partners are reluctant to share the necessary, but sensitive data about stock levels, prices and forecasts. This is due to inherent risks associated with exposing this private data.

This project proposes to use secure computation to overcome this data sharing problem in supply chain management and enable the secure collaboration and interoperation of supply chain partners **to gain the advantages of knowledge-based collaborative supply chain planning, forecasting, benchmarking and management**. We are extending existing techniques to a more elaborate setting: for the **use case of an airplane manufacturing organization** where several mutually distrustful SMEs need to collaborate in a partially integrated supply chain. We started by defining the requirements and necessary computations for the use case. We then extended the theoretical results to cover the cases of these computations if they did not exist already. Such a result is a protocol enabling this computation as part of a tool for generating the new knowledge of the computation result and managing the existing knowledge of the collaborating partners, such that it remains private. Based on the theoretical foundation we developed a prototype to evaluate the practical performance of the protocols.

In parallel to the technical implementation track, the business track identified the obstacles for the technology to be exploited. We identified the criteria for user acceptance of the technology and a benefit distribution model needs to be developed, such that all partners in the supply chain share the profit in a fair manner. The results of the business and technical track were combined when it came to building the demonstration of the results.

PILOTS WITH INDUSTRY

We piloted the prototype as part of the airplane manufacturing supply chain. We particularly implemented a system for a specific shroud nozzle which is expensive to replace when out-of-stock.

COMPANY TAKE-UP

The intellectual property developed as part of SecureSCM lead to **several patent applications in secure collaborative supply chain management generating a leading position for the world's largest business software manufacturer SAP**. SAP also ran an entrepreneurial effort to establish a new product as part of SAP Research's Next Big Thing strategy. The technology developed in SecureSCM was also used as part of bids for public tender in SAP's custom development organization.



SPACIOS

Secure Provision and Consumption in the Internet of Services

GOALS & STRATEGIES

The vision of the Internet of Services (IoS) entails a major paradigm shift in the way ICT systems and applications are designed, implemented, deployed and consumed: they are no longer the result of programming components in the traditional meaning but are built by composing services that are distributed over the network and aggregated and consumed at run-time in a demand-driven, flexible way. In the IoS, services are business functionalities that are designed and implemented by producers, deployed by providers, aggregated by intermediaries and used by consumers. However, the new opportunities opened by the IoS will only materialize if concepts, techniques and tools are provided to ensure security.

State-of-the-art security validation technologies, when used in isolation, do not provide automated support to the discovery of important vulnerabilities and associated exploits that are already plaguing complex web-based security-sensitive applications, and thus severely affect the development of the IoS. Moreover, security validation should be applied not only at production time but also when services are deployed and consumed.

Tackling these challenges was the main objective of the SPaCIoS project, which aimed to lay the technological foundations for a new generation of analyzers for automated security validation at service provision and consumption time, thereby significantly improving the security of the IoS. In particular, to achieve these challenges, **SPaCIoS aimed to develop and combine state-of-the-art technologies for penetration testing, security testing, model checking and related automated reasoning techniques, model inference, model extraction and automatic learning.** Hence, the main objectives of SPaCIoS were:

1. The development of
 - a. techniques for property-driven security testing, a variant of testing that applies techniques that make security properties (e.g., confidentiality and authentication) testable,
 - b. techniques for vulnerability-driven testing, where tests or test strategies are derived from vulnerabilities (e.g., XSS) that are likely to invalidate the security goals,
 - c. techniques for model inference/extraction from the behavior or code of the implementation, and
 - d. model checking and related automated reasoning techniques that take in input a model of the system under validation (SUV), the security goals and a model of the attacker and generate test cases to be applied on the SUV.
2. The implementation and integration of all these techniques into the SPaCIoS Tool, whose architecture is depicted in the figure.
3. The application of the SPaCIoS Tool as a proof of concept on a set of security testing problem cases drawn from industrial and open-source IoS application scenarios, in order to pave the way to transferring project results successfully to industrial practice (e.g., to SAP and SIEMENS business units) and to standardization bodies and open-source communities.

RESULTS

The SPaCIoS project has developed a set of techniques for property-driven security testing, a variant of testing that applies techniques that make security properties (e.g., confidentiality and authentication) testable, a set of

Coordinator

University of Verona (IT)

Partners

ETH Zurich (CH)

Polytechnic Institute of Grenoble (FR)

Karlsruhe Institute of Technology (DE)

Technical University of Munich (DE)

University of Genoa (IT)

SAP (DE)

Siemens (DE)

Institute e-Austria Timisoara (RO)

SPACIOS

Call 5 3 Years
(2010-10-01 to 2014-01-31)

9 Partners

5 Countries

€ 3.610.000 EU Contribution

<http://www.spacios.eu>

techniques for vulnerability-driven testing, where tests or test strategies are derived from vulnerabilities (e.g., XSS) that are likely to invalidate the security goals, and a set of techniques for model inference/extraction from the behavior or code of the implementation, as well as automated support for these testing activities: test cases are generated with model checking and related automated reasoning techniques, applied to a model of the system under validation (SUV), the security goals, and a model of the attacker. These techniques have all been implemented and integrated into the **SPaCIoS Tool**. Given a formal description of the SUV, the expected security goals, and a description of the capabilities of the attacker, **the Tool automatically generates and executes a sequence of test cases on the SUV through a number of proxies** (e.g., http-proxies). The description of the SUV can be provided directly in input by the security analyst, who can also freely choose to make use of the other entry points of the Tool by providing the SUV source code, remote access to the SUV implementation or just an attacker model.

We have implemented the SPaCIoS Tool by integrating the different components as Eclipse plugins. Moreover, we have carried out an **integration process for achieving interoperability of the SPaCIoS Tool with the NESSoS SDE platform**, and we developed tutorials and videos allowing the users to rapidly learn how to use the SPaCIoS Tool and its components. We have applied the tool as a proof of concept on a set of security testing problem cases drawn from industrial and open-source IoT application scenarios, thereby paving the way to transferring project results successfully to industrial practice (e.g., to SAP and Siemens business units) and to standardization bodies and open-source communities. We have collected the lessons learned and best practices to provide a stepping stone for similar integrations in other industrial environments.

We have transferred the results of SPaCIoS in educational activities within industry, universities, working groups or standardization organizations. We have given a number of specific presentations and organized three meetings with the Expert Group of the project and two "SPaCIoS Technology Migration Workshops". These events were specifically targeted to service designers, developers, and integrators from industry and standardization bodies in which methods, techniques, tools, case studies, and success stories developed within the project have been publicly presented.

The project participants produced more than 80 papers published or currently in print about the project's foreground. Almost 10 PhD theses on project-related research have been written, and **4 patents have been filed**. Foreground and other information related to SPaCIoS have been presented in more than 75 talks, presentations and demos by project participants. Moreover, SPaCIoS has supported or been involved, through the participants, in 101 scientific events about topics directly related to the project.



TABULA RASA

Trusted Biometrics under Spoofing Attacks

OBJECTIVES

In recent years we have seen face, voice and fingerprint identification software move from Sci-Fi films into real life affordable devices, such as smart-phones and tablets. The TABULA RASA consortium, which is supported by EU research and innovation investment, has set out to identify just how well this new software works, in particular **against the growing phenomenon of "spoofing"** i.e. using everyday materials such as make-up, photographs and voice recordings to subvert or directly attack biometric systems.

The TABULA RASA project will address some of the issues of direct (spoofing) attacks to trusted biometric systems. This is an issue that needs to be addressed urgently because it has recently been shown that conventional biometric techniques, such as fingerprints and face, are vulnerable to direct (spoof) attacks.

'A Spoofing attack', explains the TABULA RASA website, 'is a situation in which a person successfully masquerades as another by presenting a counterfeit biometric evidence of a valid user and thereby gaining illegitimate authentication. It is a direct attack to the sensory input of a biometric system and the attacker does not need previous knowledge about the recognition algorithm.' Direct attacks are performed by falsifying the biometric trait and then presenting this falsified information to the biometric system, one such example is to fool a fingerprint system by copying the fingerprint of another person and creating an artificial or gummy finger which can then be presented to the biometric system to falsely gain access.

This issue affects not only companies in the high security field but also emerging small and medium sized enterprises (SMEs) that wish to sell biometric technologies in emerging fields.

In particular the TABULA RASA project will:

- Address the need for a draft set of standards to examine this problem;
- **Propose countermeasures such as combining biometric information from multiple sources;**
- Examine novel biometrics that may be inherently robust to direct attacks.

The first issue of a draft set of standards will be addressed by analyzing the effectiveness of direct attacks to a range of biometrics, this will provide an insight as to how vulnerable the different biometric traits are to these attacks.



Coordinator

IDIAP Switzerland

Partners

University of Southampton (UK),
Starlab Barcelona (ES),
KeyLemon (CH),
Morpho (FR),
Autonomous University of Madrid (UAM) (ES),
Biometry.com (CH),
University of Oulu (FI),
EURECOM (FR),
CSSC (IT),
Chinese Academy of Sciences (CASIA) China,
University of Cagliari (IT)

TABULA RASA

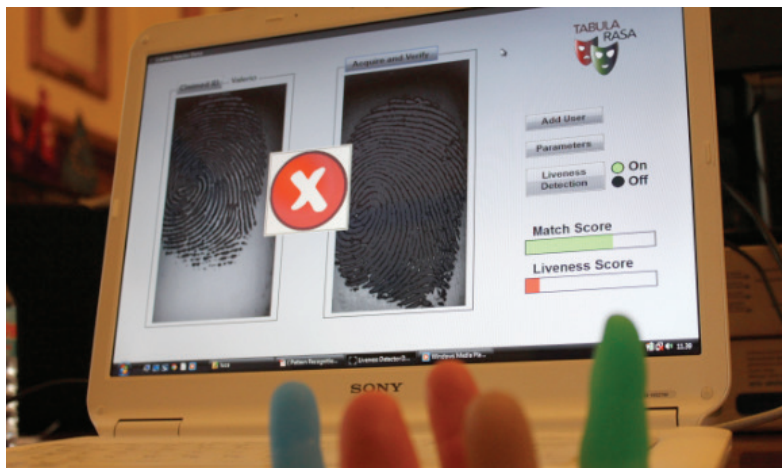
Call  4 Years
(2010-11-01 to 2014-04-30)


12 Partners


9 Countries


€ 4.038.504 EU Contribution

<http://www.tabularasa-euproject.org> 



The second issue of countermeasures will be explored in two lines, the first line of work proposes to combine multiple biometric traits to build a single system that is robust to direct attacks and the second line of work proposes to examine novel methods to perform liveness detection. Finally, novel biometrics which might be inherently robust to direct attacks, such as gait (the manner in which someone walks), vein or electro-physiological signals (such as the heartbeat), will be explored to determine their advantages and limitations.

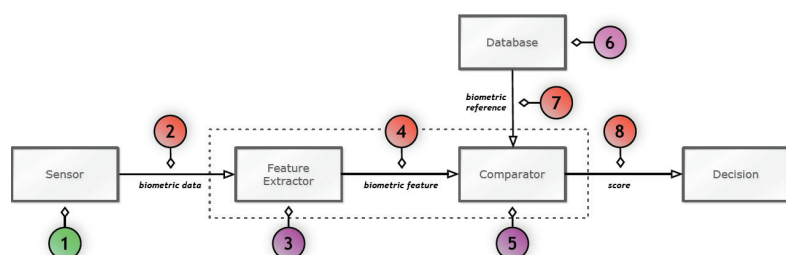
LESSONS FROM TABULA RASA

- **Vulnerability to spoofing:** TABULA RASA has shown that the most accurate biometric systems are also often the most vulnerable to spoofing.
- **Countermeasures to spoofing (anti-spoofing):** TABULA RASA has shown that anti-spoofing measures decrease the vulnerability of the biometric systems to spoofing attacks.
- **Usability:** TABULA RASA has shown that anti-spoofing measures decrease the vulnerability of the biometric systems to spoofing attacks but at the price of increased False Reject Rates (FRR).
- **Generalization:** TABULA RASA has shown that current countermeasures don't generalize yet to unseen attacks or to new realization of known attacks.

MARKET INVOLVEMENT

The project is expected to create jobs within the European SME sector as the results are integrated into commercialised solutions. For example, KeyLemon, a Swiss based start-up, has integrated a face recognition software countermeasure, developed by TABULA RASA, into a final product.

The expertise developed in the TABULA RASA project helped KeyLemon to secure a series A investment of \$1.5M, creating jobs within the company. Morpho (Safran), the world leader in biometric solutions, is also deeply involved, bringing its invaluable expertise and market vision to the consortium.





WSAN4CIP

Wireless sensor networks for the protection of critical infrastructures

GOALS, RESEARCH ACTIVITIES AND RESULTS

Critical infrastructures (CI) - energy distribution networks - but also automation control systems used to monitor Critical Infrastructures can be considered to be the nervous system of our societies. As long as everything works fine, we do not notice them, but in case of failures we suffer largely. In the last years it became apparent that CI is not only at risk from natural disasters but might also be attacked by malicious individuals. The Stuxnet incident clearly showed that automation control systems are vulnerable to attacks. An even more impressing attack was shown in the US. Here the control software of an electricity generator was manipulated so that the generator was destroyed physically.

The goal of WSAN4CIP was to substantially advance the technology of Wireless Sensor and Actuator Networks (WSANs) beyond the current state of the art and to apply this technology to the Protection of Critical Infrastructures.

The WSAN4CIP project researched innovative schemes for improving security and dependability of wireless sensor and actuator networks (WSANs) that provide low cost means to enhance CI with additional monitoring capabilities and which are by design pretty resilient against partial damage as it might be caused by natural disasters.

WSAN4CIP has followed a holistic approach in which the research topics ranged from protection of individual nodes, **via improved reliability of protocols up to middleware approaches and integration into SCADA systems.** Besides research individual aspects in all these fields also the issue of proper design of a WSAN was investigated to support engineers when planning new WSANs. The project achieved very good scientific and technical results in all of the mentioned research fields and succeeded in integrating almost all individual solutions into a set of demonstrators. **Two of these demonstrators are deployed in real working environments i.e. in a substation of the electricity distributor EDP in Portugal and along a drinking water pipeline in east of Germany.**

Beneath its strong devotion to research WSAN4CIP put significant effort in exploring exploitation opportunities. Here the strong commitment to exploitation of all partners needs to be acknowledged. All partners including the academic partners have defined an exploitation strategy which by far most cases includes economic exploitations.

In addition the project has an extremely successful dissemination record consisting of 58 publications, 21 project presentations, **3 patent applications and 1 successful contribution to IETF standardization.**



WSAN4CIP demonstrator in a substation of the electricity distributor EDP in Portugal

Coordinator

Eurescom (DE)

Partners

IHP Innovations for High Performance Microelectronics (DE),
NEC (DE),
INOV (PT),
EDP (PT),
Budapest University of Technology and Economics (HU),
INRIA Rhone-Alpes (FR),
Lulea University of Technology (SE),
Sirrix (DE),
Tecnatom (ES),
University of Malaga (ES),
Frankfurt Water Company (DE)

WSAN4CIP

Call 7 3 Years
(2009-01-01 to 2011-12-31)

13 Partners

6 Countries

€ 2.775.000 EU Contribution

<http://www.wsan4cip.eu>

2

**INNOVATIVE PROJECTS
WORKING TOWARDS
THE MARKET**





ASPIRE

Advanced Software Protection: Integration, Research and Exploitation

Coordinator

Ghent University (BE)

Partners

Fondazione Bruno Kessler (IT)

Gemalto (FR)

NAGRA Kudelski (CH)

Politecnico di Torino (IT)

SafeNet (DE)

University of East London (UK)

ASPIRE

Call  3 Years
(01.11.2013 – 31.10.2016)



7 Partners



6 Countries



€ 2.949.977 EU Contribution



<http://www.aspire-fp7.eu>

«I think it's very important for EU ICT security industry to make a switch from hardware protection, which is currently a strength point, to software protection, which is a weakness.

Mostly American companies start dominating the video content delivery market, and if we do not find a way for European companies to deliver content in a protected manner, we are going to be blown away». Bjorn De Sutter

Traditional sensitive content and software protection mechanisms are based on hardware, but such approaches are not convenient for the mobile devices today. **ASPIRE is going to introduce novel software-based protection mechanisms for mobile devices**, which will also be useful in the context of expensive software license checking or remote content delivery. **The software-based protection mechanisms of ASPIRE will be more user-acceptable than hardware-based protections**, while being cross-platform and less expensive than hardware-based protections. The project explores a range of obfuscation techniques, white-box cryptography, remote attestation and various other anti-tampering mechanisms as the main protection techniques. One of the goals of ASPIRE is to enforce renewability by guaranteeing that all deployed protection mechanisms can be updated in the field on a regular basis.

INNOVATION ACHIEVEMENTS

ASPIRE works on the following main results:

- An integrated tool chain for software-based protection mechanisms;
- A decision support system for the tool chain that will be able to recommend the best protection strategy to non-expert users based on the tool version and the assets to be protected;
- A knowledge base based on empirical studies and software metrics that will include a set of attacker models for software systems and economic models for these attackers.

OVERCOMING CONSTRAINTS OF THE MARKET

Today's business models of software distribution for mobile devices typically do not support selective provisioning of software to customers: each customer gets the same version, while the ASPIRE results to some extent assume that each software copy distributed to a customer may be different. The project aims for demonstrating that the protection advantages outweigh potential disadvantages of such software distribution models.

Another potential hindrance is the perception of trusted technologies today. Even if some protection mechanism, e.g., an obfuscation algorithm, works in practice, its trustworthiness cannot be demonstrated by, for example, using Common Criteria. Thus businesses might prefer to stick to the traditional schemes in case the project fails to clearly demonstrate what level of protection its technologies provide.

A more general problem highlighted is related to the perception towards the software protection in the case of legal requirements: as explained by the coordinator: "The European ICT industry relies on very strong protection: for example, we use the more secure smart cards in our credit cards, while in

America they still rely on the insecure magnetic stripe. Their business models don't depend that much on security [...] But many European businesses really do rely on it, for making profits, for avoiding detrimental damage from illegitimate attacks, and for meeting legal requirements. Nevertheless, we are not ready really to move to software-only protection. The ASIPIRE project wants to address that by providing strong, measurable protections. With hardware and with crypto – that's done. For software protection it's not yet possible, software protection is now incompatible with many business models and legal requirements. So we want to bridge that".

ASIPIRE dedicates itself to thorough evaluation of the protection levels its technologies provide. This evaluation includes experiments with students, security consultants and real hackers that will allow understanding how secure and reliable the protections are. At the same time, the industry partners in ASIPIRE see business cases for the ASIPIRE results – and they will work on business acceptance.

MARKET INVOLVEMENT

Software-based protection mechanisms for sensitive content and code are easier to deploy than hardware-based protections. The end-users will have more options for protection, while Europe can gain market leadership in this area and in the linked business areas (e.g., remote content provisioning and video streaming).

USE CASES

ASIPIRE wants to push the deployment of protection technologies on real world applications based on the real protection they provide, as stated by the coordinator: *"How do you model how much an attack will be delayed if you deploy some protection? There exist no formal models, and no real practically useful models. So we are going to do experiments with people and experiments with tools that attackers use, to try to measure how protections can influence the attacks, how much they actually delay the attacks [...]. How to model the relations between the protections and the attacks, and which protections are really going to protect against certain attacks. Just the fact that we hopefully be able to reason about the real, practical strength of protections, not just say things in theory, but **really have the foundations to say that this protection is better than that protection**".*

The project then has planned to carry out three case studies: content delivery, software licensing, and one-time passwords. In each case study, the protection technologies delivered by ASIPIRE will be applied to, and validated on an application representative of software used in real-world business domains. Moreover, **one additional application (currently the candidate is an online game engine) will be developed and protected by the ASIPIRE tools, and a public competition for attacking it will be launched.**



AU2EU

Authentication and Authorisation for Entrusted Unions

Coordinator

Eindhoven University of Technology (NL)

Partners

Philips Electronics (NL),
Bicore Services (NL),
Macquarie University (AUS),
Edith Cowan University (AUS),
NEC Europe (UK),
Commonwealth Scientific and
Industrial Research Organization (AUS),
Royal Melbourne Institute of Technology (AUS),
IBM Research (CH),
Thales Communications and Security (FR),
University of New South Wales (UK),
German Red Cross (DE)

ABC4Trust

Call  2 Years
(01.12.2013 – 30.11.2015)



12 Partners



6 Countries



€ 2.950.000 EU Contribution



<http://www.au2eu.eu/>

AU2EU is an EU-funded collaborative research and development project that brings together a strong collaboration of leading industry and research organisations from Europe and Australia, determined to increase trust, security and privacy.

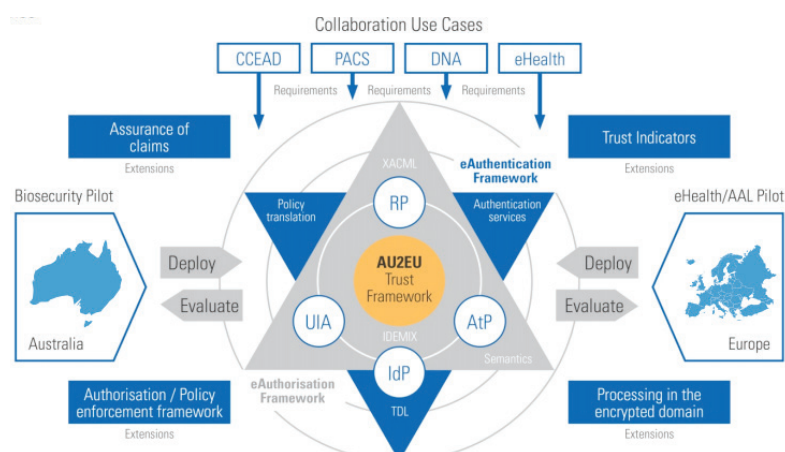
OBJECTIVES

The AU2EU project aims at **fostering the adoption of security and privacy-by-design technologies in European and global markets**. The project will contribute to increased trust, security and privacy, which in turn shall lead to increased adoption of (cloud-based) critical infrastructures and collaborative delivery of services dealing with sensitive data. **The project will design a joint eAuthentication and eAuthorisation framework for cross-domain and jurisdictional collaborations**, supporting different identity/attribute providers and organisational policies and guaranteeing privacy, security and trust. Central to the AU2EU project is the implementation and demonstration, in a real-life environment, of an integrated eAuthentication and eAuthorisation framework. **Two pilots** are executed to demonstrate feasibility of our approach for two of the use cases, i.e. for the **bio-security** the incident response use case in Australia and the collaborative services for **eHealth** and the Ambient Assisted Living use case in Europe.

ACTIVITIES

The AU2EU objectives will be achieved by the following activities

1. designing a joint eAuthentication and eAuthorization framework for cross-domain and jurisdictional collaborations, supporting different identity/attribute providers and organizational policies and guaranteeing privacy, security and trust;
2. advancing the state-of-the-art by extending the joint eAuthentication and eAuthorization framework with assurance of claims, trust indicators, policy enforcement mechanisms and processing under encryption techniques to address specific security and confidentiality requirements of large distributed infrastructures;



3. implementing the joint eAuthentication and eAuthorization framework as a part of the platform that supports collaborative secure distributed storage, secure data processing and management in the cloud and offline scenarios;
4. deploying the designed framework and platform in two pilots on bio-security incident management and collaborative services in Australia and on eHealth and Ambient Assisted Living in Europe; and
5. validating the practical aspects of the developed platform such as scalability, efficiency, maturity and usability.

The AU2EU project is progressing to the plan, the integrated authentication and authorization platform is developed and the two pilots are being deployed.

ADDED VALUE

The aforementioned activities will contribute to the increased trust, security and privacy, which in turn shall lead to the increased adoption of (cloud-based) critical infrastructures and collaborative delivery of services dealing with sensitive data. AU2EU strategically invests in two pilots deploying the existing research results as well as the novel techniques developed in the project to bridge the gap between research and market adoption.

The project builds on existing schemes and research results, particularly on the results of the ABC4Trust project as well as the Trust in Digital Life (TDL) initiative, which initiated this project and will support its objectives by executing aligned activities defined in the TDL strategic research agenda.

The project brings together **a strong collaboration of leading industry** (such as Philips, IBM, NEC, Thales), **SMEs** (such as Bicare) **and research organizations of Europe** (such as Eindhoven University of Technology) **and Australia** (such as CSIRO, Edith Cowan University, RMIT University, University of New South Wales & Macquarie University) **as well as the large voluntary welfare association** (such as German Red Cross).

The consortium is determined to make a sustained long term impact through commercialization, open source & standardization of open composable infrastructure for e-services where privacy and interoperability with existing technologies are guaranteed.



Towards a confidential and compliant cloud

COCO CLOUD

Confidential and Compliant Clouds

Coordinator

HP Italiana (IT)

Partners

Grupo Hospitalario Quiron (ES)

Oslo university (NO)

Bird & Bird LLP (UK)

SAP (DE)

Imperial College (UK)

Agenzia per l'Italia Digitale (IT)

Atos (ES)

Consiglio Nazionale delle Ricerche (IT)

COCO CLOUD

Call  3 Years
(01.11.2013 – 31.10.2016)



9 Partners



5 Countries



€ 2.799.867 EU Contribution



<http://www.coco-cloud.eu/>

While Cloud Computing today is widespread, many concerns remain regarding security of the sensitive data stored in the Cloud. Especially if these data need to be exchanged with other users or updated across many user devices. Ensuring confidentiality, integrity and availability of the data remains problematic with the current cloud computing services offered.

Confidential and Compliant Clouds (Coco Cloud) aims at designing a confidential and compliant cloud for Europe allowing cloud users to securely and privately share their data in a cloud environment.

The main goal of the project is to **enable seamless sharing of information among the users and across the cloud and various mobile devices**, while keeping the data confidential and executing the data sharing in compliance with the data sharing agreements.

INNOVATION ACHIEVEMENTS

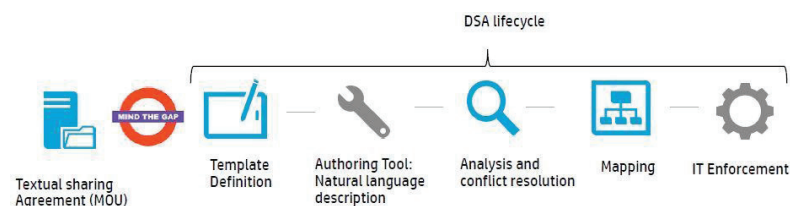
There is a gap between a traditional legal contract regulating the data sharing and the software infrastructure supporting it. Coco Cloud aims at making progress towards filling the gap through the **usage of so called electronic Data Sharing Agreements (DSAs)** and enforcing them. Basically the aim of DSA is to capture the data sharing policies that restrict both suppliers and consumers of data and govern the flow of data between them.

Taking a “compliance by design” approach, the Coco Cloud places an early emphasis on understanding and incorporating legal and regulatory requirements into the data sharing agreements which are key challenges for legally compliant data sharing in the cloud.

The project provides a flexible, legally compliant framework for secure data exchange between end-users and takes account of legal and business requirements for the creation, analysis, operation, and termination of DSAs.

In summary, Coco Cloud project delivers:

- A secure end-to-end data sharing infrastructure from data repository to user device (mobile or fixed) and vice-versa;
- A data sharing agreement authoring tool, with legal and business compliance ensured by design (starting from the reutilization of the main outcome of the CONSEQUENCE project) leveraging on predefined ontologies;
- An approach to define data sharing policies in natural language.



DSA Lifecycle

OVERCOMING CONSTRAINTS OF THE MARKET

What usually happens currently, when end-users data are going to be processed by organizations, is that end-users are asked to accept online a series of regulatory clauses on the terms of data processing. Furthermore, end-users find it difficult to understand these terms and conditions and

how to express their potential preferences in terms of data sharing and handling.

This introduces burdens on users and usability issues of proposed solutions for end-to-end automation of contract definitions and their enforcement. Another key problem relates to trust.

In general, there is no guarantee that contracts will be fulfilled and that potential violations will be promptly identified. Violation detections require verification of organizational practices, auditing and accountability frameworks. Furthermore, these contracts could evolve so they need continue adaptation, for example due to changes of provisioning of services, legislation, preferences, etc. This requires lifecycle management of contracts.

Since user acceptance is a potential concern for Coco Cloud results exploitation, **one of the main goals of the project is contributing to solve the specific problem of how to provide more automation in the definition and enforcement of data sharing contracts.**

Another concern is the missing regulation for data privacy in Europe. The project requires more homogeneous system for privacy across the Member States to facilitate deployment of its technology.

The project includes two partners that are legal experts. Their work is dedicated to ensuring legal compliance of the data sharing process and to monitoring the EU legal framework for privacy in order to propose the best strategy for the Coco Cloud framework deployment across Europe.

Eventually, to simplify service delivery, lower operational risk and optimize workload across Cloud Providers, **the Coco Cloud framework will be hosted on a secure, open, flexible HP CloudOS platform based on OpenStack technology.**

MARKET INVOLVEMENT

Companies are hosting a growing amount of confidential documents, subject to external obligations and regulations. Very often this data needs to be shared among partners, customers or legal agencies. The current platform for sharing this data is shifting to Cloud data storage, raising worries about data protection and data usage control.

Coco Cloud solves these concerns by allowing end-to-end data protection through multilateral data sharing agreements and a legal complaint-by-design approach to ensure secure document storage and exchange in the Cloud.

Secure and private data sharing will increase user trust in cloud services and ultimately increase the widespread adoption of cloud computing. Greater use of cloud computing will have benefits for users and for the digital economy in general. Trustworthy European clouds will have a competitive advantage over the less trusted clouds of the competitors, as after the revelations by Edward Snowden, for many users the trust in secure handling of their data by cloud companies has eroded.

PILOTS

In order to have the widest possible view over the context in which the new framework will operate, **the three pilots come from unrelated domains will be implemented.** The first pilot regards the **sharing of patients' medical/health data between patients and among different doctors**, possibly operating in different hospitals. The second pilot comes from the Public Administration sector, and refers to **the securely exchange data regarding citizens between public administrations.** The third pilot involves **the fruition of confidential corporate business data by employees from mobile devices.**

In particular:

1. The eHealth pilot assigned to GHQ partner from Spain, which aims to provide a cloud-based patient and doctor radiology portal that facilitates the ubiquitous interaction of the patients and the medical specialists with the medical imaging departments by means of sharing highly sensitive medical data such as medical images and their corresponding reports;

2. The eGovernment pilot, attended by AGID from Italy, implemented in the eGovernment environment in order to provide a cloud service that enables the sharing of civil data of citizens (i.e. the vital events of citizens) between and across different Italian Public Administrations (PA);

3. The mobile pilot, managed by SAP from Germany, which is about the corporate data treatment and the consumption of confidential information on a mobile environment.

The Coco Cloud platform will be validated on a generic sample application in an industrial test bed, whose responsibility is on HP. The test bed hosts the development and tests environment and it is the deployment environment to run the use-cases defined by the pilots in order to show basic business case scenarios.

REFERENCES & COLLABORATIONS

Coco Cloud is collaborating with A4Cloud for the definition and investigation of technical solutions in order to translate and instantiate data protection and contractual policies (e.g. Data Sharing Agreement and Privacy Level Agreement) to machine-readable policies.



ENVIROFI

The Environmental Observation Web and its Service Applications within the Future Internet

Coordinator

ATOS (ES)

Partners

University of Southampton (UK)
JRC EC (BE)
Austrian Institute of Technology (A)
SINTEF (N)
NILU (N)
Eurescom (DE)
UBIMET (A)
Umweltbundesamt (EAA) (A)
IOSB at Fraunhofer (DE)
CNR (IT)
Marine Institute (IRL)
InTune (IRL)
Aalto University (FI)

ENVIROFI

Call  2 Years (2011-04-01 to 2013-03-31)
(extended to 2013-06-30)



Partners



Countries



€ 4.963.942 EU Contribution



<http://www.envirofi.eu>

PROJECT CONTEXT AND OBJECTIVES

ENVIROFI is a co-funded research project within the Future Internet Public Private Partnership (FI-PPP) programme of the EU's Seventh Framework Programme (FP7). The project is dedicated to the environmental usage area of the Future Internet. It will explore environmental enablers (applications for collecting and processing environmental data) and provide environmental sector requirements to FI-WARE, the FI-PPP core platform project. Thus, ENVIROFI will lay the foundation for an environmental observation web, which will help Europe tackle the grand societal challenges of climate change, environmental degradation, and sustainable growth.

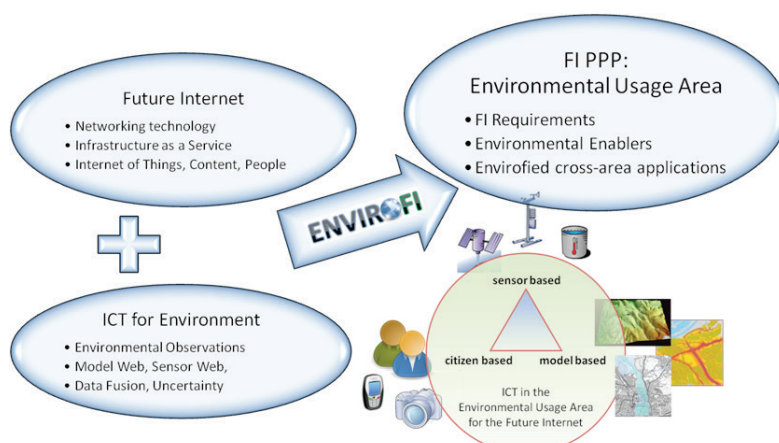
ENVIROFI's vision is to establish an Environmental Observation Web in which all environmental data, whether from sensors, citizens, or models, are available anytime anywhere through the Internet in a standardised, usable format.

ENVIROFI specifically works on three environmental application areas: **personalised atmospheric data, marine assets, and biodiversity**. We envisage a system with dynamic understanding of the Earth's atmospheric, marine and terrestrial spheres for the benefit of all European citizens.

So far, no standardised Europe-wide, cross-domain and web-enabled solution for capturing, storing, processing and visualizing the avalanche of observation sources exists. Reasons for this unsatisfactory situation can be traced back both to shortcomings of the available technology, and to the parallel evolution of information systems and data models across geographic and usage areas.

Thanks to the diversity of stakeholders and strong involvement of the key ICT industry players, the FI-PPP is in the position to address both issues and: (1) develop advanced technical solutions beyond the reach of environmental area alone; as well as (2) help establishing the observation-related and geospatial standards in usage areas currently relying on non-standard and proprietary solutions.

In order to succeed, ENVIROFI intended to assure the existing environmental resources can be used in cross-domain applications, while at the same time assuring the environmental applications can profit from FI developments.



The key challenge for ENVIROFI was therefore to assure the FI architecture is compatible with standards, best practices as well as existing and upcoming infrastructures of the environmental usage area. In order to overcome this challenge, the ENVIROFI team had to (1) understand the needs and architectural constraints of FI-WARE and of the other usage area projects; (2) share knowledge with all FI-PPP participants on generic standards and best practices which were developed within the environmental usage area; and (3) inform the environmental usage area community of the advanced functionality developed within the FI-PPP. An additional challenge was the introduction of volunteered geographic information (VGI) and information from low-quality sensors as additional sources of observations.

These community-generated environmental observations represent a wealth of information which is currently unused and therefore in need of integration with other fragmented data and information sources, traditionally managed by research and educational institutions and industries.

ENVIROFI leads the way in showing how a future internet ICT infrastructure which support geospatial information in Europe enables European Communities, such as environmental policy makers, scientists and social communities collectively monitor, manage and protect their environment. **ENVIROFI aimed to make information management standards, services and resources more accessible to the wider Eu-ropean communities in context of the Future Internet environmental usage area and beyond.** It will also lay the foundations for a Pan European environmental observation web with the following achievements:

- identifying and implementing environmental enablers operating in a multi-style Service Oriented Architecture (SOA);
- implementing reusable knowledge management services for the marine, land and atmospheric usage domains and beyond;
- enabling the wide communities to access to environmental sensing from various sources with context and situation aware spatial information;
- providing on-demand integrated information to large, communities and industries operating in diverse market sectors, such as the environmental energy and the leisure sector.

ENVIROFI APPROACH

ENVIROFI worked on **three use case scenarios: biodiversity, human/environment interaction, and collaborative usage of marine data.**

1. *Bringing Biodiversity into the Future Internet (enabled biodiversity surveys with advanced ontologies; analysis, quality assurance and dissemination of biodiversity data)*

In terms of phenomena on the land, we focus on terrestrial biodiversity. The UN Convention on Biodiversity (CBD) and the EU have set a new target of halting the loss to biodiversity by the year 2020. In order to meet this goal we must first provide a solid basis upon which to judge this progress. Observational data on biodiversity must be merged from all available sources while assuring high quality. Using outreach groups for data survey, we can greatly widen the base from which observational data may be gleaned. Scenarios on biodiversity occurrence illustrate the use of humans supported by mobile devices such as smart phones as the main 'sensor' for data provision.

2. *Personal Information System for air pollutants, allergens and meteorological conditions (enhance human to environment interaction; atmospheric conditions and pollution in "the palm of your hand")*

On the atmospheric sphere, we concentrate on individualized exposure assessment. Today, we have easy access to a great deal of information via television, radio and the World Wide Web. This includes pollution, pollen and meteorological data which are all relatively easily accessed in one or more dissemination channels. All this data contributes to a common sense,

but it is not tailored to individual user needs. Relevancy of data and interpreting it are key issues for users today, especially with regards to pollen and pollution. Future eEnvironment services shall therefore aid the users towards in tailoring information relevant to their individual requirements.

3. *Collaborative Usage of Marine Data Assets (assess needs of key marine user communities; selection of representative marine use cases for further trial: leisure and tourism, ocean energy devices, aquaculture, oil spill alert)*

For the marine domain, the challenge for research and innovation is to create synergies with the market and with policy needs that are necessary to deliver significant value added to Europe from its vast marine resources. Enabling technology platforms are currently deployed across a range of existing marine related sectors including shipping, security and logistics, environmental monitoring and offshore energy. Next generation decision based management tools have to dissolve national borders. They shall address these developments in respect to distributed sensing, and wireless and cable communications.



A new methodology to model cyber security

INTER-TRUST

Interoperable Trust Assurance Infrastructure


Coordinator

Softeco Sismat (IT)

Partners

Montimage (FR)
Telecom Bretagne (FR)
Telecom SudParis (FR)
University Rovira I Virgili (ES)
Search-Lab (HU)
University of Malaga (ES)
University of Reading (UK)
University of Murcia (ES)
SCYTL (ES)
INDRA (ES)

INTER-TRUST

Call  3 Years
(2012-11-01 to 2015-04-30)



11 Partners



5 Countries



€ 3.750.000 EU Contribution



<http://www.inter-trust.eu>

«I think it would be worthy to focus more on usability. And the next step would be to extend the demonstrations. We have two iterations, but of course more are needed to achieve the results that are really usable in the market. I am working for a company, not a research institute, and we are mostly interested in having results concretely usable».

Enrico Morten, project coordinator.

The INTER-TRUST project aims to **design a dynamic and scalable framework to support creating and deploying critical services and applications, which can autonomously adapt to various security, privacy, interoperability, legal, social and economic requirements.**

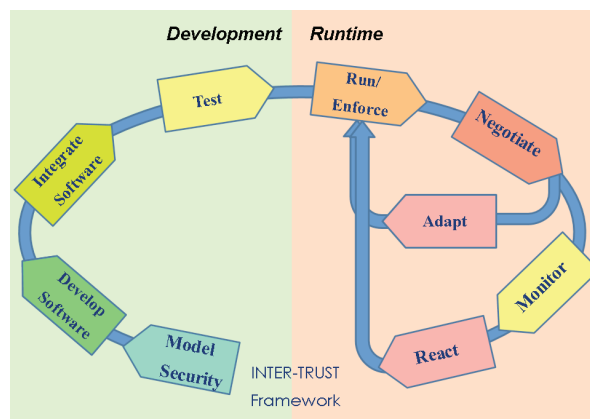
One of the main objectives of INTER-TRUST is a new methodology to model cyber security, the Organisation Based Access Control Model (OrBAC). The project also works on a **new negotiation mechanism, based on Service Level Agreements, to negotiate security between parties in Internet, including methodology and tool support.**

The INTER-TRUST framework aims to be highly dynamic; thus the project develops also a methodology to assure the required dynamicity of the framework, including software support and guidelines. To assure that that overall system is trustworthy, the project also designs new monitoring tools to assess security in the dynamic environments.

VALIDATION STRATEGY

The project works with **two case studies in the intelligent transportation systems** (INDRA company), in the context of vehicle to vehicle communication, and **the e-voting domain** (SCYTL company): "These are the direct customers of the results of the project, so they are involved directly. Also they are planning and are already doing some economic evaluation about the viability and usability of the project results, it is part of their exploitation plan". (Enrico Morten)

Two iterations of the validation process are planned for each use case, aligning with the standard software development approach: requirements, prototyping, testing, and assessing the end-user feedback.



The INTER-TRUST software framework and its development cycle

HAVE A LOOK AT

The project has conducted a market study to assess the market for provision of network security advisory and mitigation services for security in service infrastructures, and more general market of trustworthy applications that might also be interested in the INTER-TRUST results.



MASSIF

MANagement of Security information and events in Service InFrastructures

OBJECTIVES

MASSIF focused on advancements in security information and event management (SIEM) systems that deal with real-time analysis of events and security alerts.

Standard SIEM systems typically are deployed at a platform layer and they do not take into account data from higher layers, such as the business process view. Being usually deployed on a single node responsible for processing all event correlation rules, they are not scalable. Moreover, existing systems are not able to react to detected attacks.

INNOVATION ACHIEVEMENTS

The MASSIF project successfully developed a next-generation SIEM framework for service level infrastructure. The MASSIF solution combines novel security technologies to provide the industry's most advanced security management solution.

MASSIF is a SIEM framework consisting of several components that provide MASSIF with its key innovative features, introduced as follows:

- Multi-domain: Clear decoupling between the target (monitored) and SIEM (monitoring) systems, for minimal impact on the observed infrastructure, and adaptation to varying target/SIEM system combinations;
- Scalable data acquisition and collection of vast amounts of events from diverse and geographically spread nodes;
- Event Authenticity and unforgeability;
- Anonymisation capability by masking the identities of individuals at data gathering;
- Distributed and near real-time aggregation, dissemination and processing of events;
- High Availability or non-compromise of events between origin points and processing nodes (distributed or central);
- Resilient operation against faults and attacks of incremental severity, maintaining availability, integrity and confidentiality;
- Scalability and elasticity of correlation, across integrated and distributed engine implementation alternatives;
- Cross-layer correlation of security events from network and security devices and service infrastructure such as correlation of physical and logical event, and multi-level security event modelling that provides a holistic solution to protect the service infrastructures;
- Predictive security monitoring that enables proactive fighting of attacks by predicting future critical states in the monitored process;
- Reaction capabilities through countermeasures selection based on an ontology-driven approach.

MARKET ACCEPTANCE GAPS

The MASSIF consortium has faced the following gaps:

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

Coordinator

ATOS (ES)

Partners

SPIIRAS (RU)

T-Systems (ZA)

Fraunhofer - SIT(DE)

Polytechnic University of Madrid (ES)

CINI (IT)

AlienVault (ES)

Faculty of Sciences of the University of Lisboa (PT)

Orange Labs - France Telecom (FR)

6CURE (FR)

Epsilon (IT)

Telecom SudParis (FR)

MASSIF

Call  3 Years
(2010-10-01 to 2013-09-30)


12 Partners


7 Countries


€ 5.950.000 EU Contribution

<http://www.massif-project.eu> 

MITIGATION STRATEGIES

The modularity of the MASSIF platform, where each component is independent from others, allows to easily reconfiguring MASSIF for each new platform. The MASSIF team overcomes consumer unawareness by demonstrating the solutions and their potential to customers, including potential customers from the project Advisory Board.

IMPACT

The modular nature of the MASSIF solution eases integration of single components or combinations into existing products or services, providing them with enhanced and trustworthy functionality, while preserving the systems legacy. This enables the MASSIF offer to be easily adapted to different customers' needs in terms of technological solution and pricing. Additionally, it allows a relatively straightforward integration with existing commercial solutions, such as OSSIM and Prelude.

MASSIF solutions proved its usability in several areas where societal aspects are usually compromised.

- **Protection against cybercrime and attacks against information systems.** Despite widespread awareness of the impact of cybercrime, cyber-attacks continue to occur frequently and result in serious financial consequences for businesses and government institutions. The cost of cyber-crimes impacts all industries but defence, utilities and energy, and financial services have a significant higher cost compared to organizations in technology, communications, public sector, transportation, retail, and consumer products. Recovery and detection are the most costly internal activities. MASSIF features such as the resilient framework, predictive security monitoring or reaction capabilities can highlight a significant cost-reduction in normal business operations.

MASSIF can detect activity associated with an attack. The MASSIF predictive security analyzer can process a behaviour analysis that can efficiently detect misuse patterns. A security analysis model is used to identify current and close-future violations of the security policy. A mapping model maps transitions in the security analysis model onto security alerts that are provided via the repository to the Decision Support and Reaction component and the MASSIF visualisation service.

An example of these capabilities is the **MASSIF application to the Olympic Games IT infrastructure**, where complex patterns are detected by MASSIF components and in reaction, new security policies are enforced.

- **Critical infrastructures Protection.** Critical Infrastructures (CIs) are already exposed to Cyber-security attacks and they will be even more so in the future. Protection of these systems against acts of cyber warfare means that citizens are safer as their compromise could impact devastatingly on economies and possibly threaten lives. Therefore the deployment of MASSIF in CIs offers citizens more robust protection against attacks on critical industrial process control systems (e.g: the critical infrastructure protection scenario). One example of this **deployment is the DaMon system over the Montecotugno dam in Italy, the largest earth-fill dam in Europe.**
- **Fight against fraud.** Fraud has always been a challenging topic. Detecting, investigating and responding to fraudulent transactions from within and outside an organization is an essential function of business operations. Innocent account holders with compromised systems inadvertently provide front door access to critical banking applications, resulting in huge losses to financial organisations and personal suffering to their customers. MASSIF can help to mitigate fraud. An example is the **Mobile Money Transfer** scenario, where MASSIF was applied successfully to detect and react against the abnormal behaviour of a fraudster (after taking over of the

victim's account) who carried out several transactions by visiting several merchants and spending the mMoney of the victim.

- **Data protection and Privacy.** Collection of security events by SIEMs is becoming more widespread. The challenge occurs where monitoring service / location may be provided by a 3rd party organisation or in a different country. While privacy requirements and approaches are well described for primary systems, it is less clear how these principles should be extrapolated to "meta-systems" like SIEMs, resulting in a privacy risk (potentially also cross-border). The Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data imposes several implications to SIEMs with regards to data protection. In MASSIF, data protection is taken care by means of the anonymization techniques, resilient storage and reliable transmission.

Privacy implications of SIEMs were early considered within MASSIF. Technical solutions such as anonymisation are available to help implement privacy in applications. An example of this **MASSIF application is the implementation of privacy-preserving data aggregation in electronic health records for the Italian Technological infrastructure of the Electronic Health Record.**

In addition, by relying on Complex Event Processing technology and on a stream-based computing paradigm, MASSIF solutions satisfy the issue by designing the "zero storage" principle. The only data which will be permanently stored is the one which might be needed for forensic use (after a security violation has been detected). In this case, data will be stored in the secure storage facility, and it will be made available only to entitled parties, according to regulations.

As a direct research result of **MASSIF Atos launched "yourCySEC" solution, a service level SIEM that is subject to several commercial actions with Atos customer, as well to use in other R&D projects, such as FI-WARE (Future Internet Core Platform) project.** Epsilon also integrated MASSIF features in the **DaMon application** (an application, for the electronic monitoring of physical systems) and in **Nex-tapps** (a cloud base platform for developing web applications)¹.

6cure is studying use of MASSIF components and use of knowledge generated in MASSIF to enhance GFI Informatique's SIEM platform VigieSI.

Fraunhofer SIT cooperated with security consultants to increase the uptake of the components Predictive Security Analyser and Trusted-MIA. Particularly, the T-MIA was evaluated by the company NCP.

On top of this it is worth mentioning that **UPM filed two patents of the parallel processing of continuous queries on data streams²**. These patents and the results related to the Complex Event processing are going to be exploited by means of a start-up called **LeanXcale** that was created in 2014. Other MASSIF components are available as open source at: <http://fitnesslab.altervista.org/index.php/it/download/source-code>.

ZOOM IN

Four industrial scenarios were used in MASSIF to prove the feasibility of the framework and its features:

- **The Olympic Games IT infrastructure deployed and managed by ATOS**, which demanded high scalability of event processing and the detection of complex behaviour patterns.
- **Orange Labs (France Telecom) provided a scenario on mobile phone-based money transfer service** facing security events, especially for the "non-IT" and "service" events. This scenario proved MASSIF process behaviour analysis, and visualization of events for forensic analysis.
- **T-Systems South Africa provided managed IT outsource services** with a high degree of complexity in setting up SIEM systems for large distributed enterprises.
- **Epsilon demonstrated the use of the advanced concepts of SIEM in an IT system supporting a critical infrastructure (dam)**, especially the convergence of physical and logical security.

¹ <http://www.epsilononline.com/index.php/component/content/category/2-non-categorizzato.html>

² References: EP2011/003011 and EP11729557.6 (<http://www.google.com/patents/US20130346446>)



The user at the focus of attention

MUSES

Multiplatform Usable Endpoint Security

Coordinator
S2 Grupo (ES)

Partners

University of Granada (ES)
HITeC at the University of Hamburg (DE)
Catholic university of Leuven (BE)
CurE (AT)
Sweden Connectivity (SE)
WiND (IT)
University of Geneva (CH)
TXT e-Solutions (IT)

MUSES

Call  8 3 Years
(2012-10-01 to 2015-09-30)



9 Partners



7 Countries



€ 3.590.339 EU Contribution



<https://www.musesproject.eu/Muses>

The MUSES project aims at improving the corporate security by focusing on the end-user -an employee- and her interaction with mobile devices.

The main goal of the project is to propose a way to enforce corporate security policies such that the user can continue her workflow and does not want to circumvent the controls.

The major contribution of the project is the **MUSES system, which is a user-centric, device-independent and self-adaptive corporate security system that is able to analyse in real time the risk and trust for user actions performed with the device**, that can be personal or owned by the company.

The MUSES system has two elements: the **MUSES server running on the company server**, and the **MUSES client installed on the employee's device**. The MUSES server is in charge of decision making on corporate security policies enforcement. The MUSES client observes the context, in which the user is working, for example, the operating system or the location, and then it acts on the server decisions on whether to accept or reject the user request.

The decision process is based on the context-aware Risk and Trust Analysis system that is monitoring whether the pair formed by the user and the device is trustworthy or not.

Other major results of the project are recommendations for usability, context-aware risk evaluation, user trust, and also the guidelines for the design of enforceable corporate policies. Legal implications are also at the core of MUSES' research and embedded into the development of the system.

RECENT DEVELOPMENTS

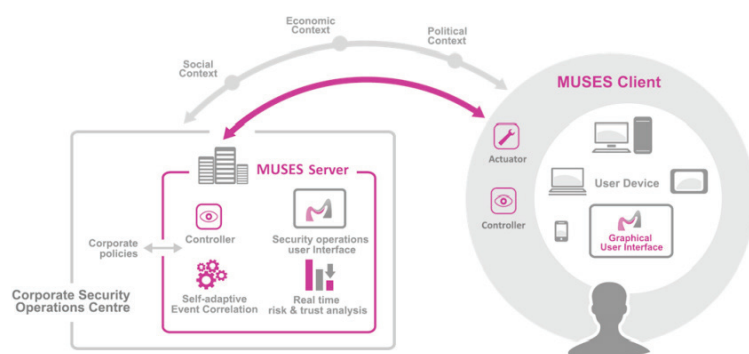
Prototype #1 (mobiles and tablets running on Android) is already implemented and being currently validated in production environment trials. Work is already under way in **Prototype #2 that will incorporate many new features to #1 and also work on other devices and OSs (e.g. laptops, Windows).**

While working on the system, the project has studied many aspects of corporate security policies relevant for mobile devices. For example, the partners have found out that many standard mobile security policies are not enforceable by design. Another recent finding is the use of opportunities. For instance, if an employee is working using an insecure connection (e.g., in an airport) but there is an opportunity for her to submit an offer to a client, the MUSES system will allow her to work. The project also works on identifying persuasive ways to enforce security, e.g., via gamification.

VALIDATION STRATEGY

MUSES is currently conducting a **first set of trials, involving actual end-users testing MUSES' Prototype #1. The end-users are persons from a Consultancy department, a CERT and a telecom**

operator. The project has designed a set of metrics to be measured during the trials, including perceived usefulness and perceived usability of the system. A similar set of trials will be run before the end of the project for Prototype #2.



HAVE A LOOK AT

<https://www.musesproject.eu> to access project Deliverables, Scientific papers, news and other items of information about MUSES.

Check also <https://github.com/MusesProject>

MUSES System

Research & Market in ICT: new hints in Horizon 2020



NECOMA

Nippon-European Cyberdefense-Oriented Multilayer threat Analysis

PROJECT OBJECTIVES

The NECOMA project addresses objective (c), Cybersecurity for improved resilience against cyber threats, of the ICT-EU Japan Coordinated call FP7-ICT-2013-EU-Japan. It aims at providing new means to understand cyberthreats and to mitigate their effect on infrastructure and endpoints. It addresses the aspects of (1) threat data collection, leveraging past and current work on the topic with the goal to expand these existing mechanisms, (2) threat data analysis, not only from the perspective of understanding attackers and vulnerabilities, but also from the point of view of the target and victim and, (3) develop and demonstrate new cyberdefense mechanisms.

INNOVATION ACHIEVEMENTS

One of the main research objectives of NECOMA is to analyze data both from an infrastructure perspective (networks and large computing infrastructures) and endpoints (smartphones and browsers). Towards that direction the consortium (i) has established mechanisms to gather information from those different layers (ii) has identified common attributes in order to easily (iii) correlate and (iv) store them in appropriate schema for further analysis. More specifically, 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. A common communication mechanism named N6¹ has been defined and applied to most of those datasets in order to provide a common interface to each other. That way we simplify the transfers of those data to the heavy analysis Hadoop based platform named MATATABI² and towards a collaborative repository for cybersecurity data and threat information on top of a privacy-aware storage system, named TAMIAS³. Research analysis on those data has led to further research achievements like a MapReduce framework for anomaly detection in backbone networks, DNS traffic analysis platform with Hadoop framework, classification of DNS erroneous queries, users' behavior analysis, classification of SSL servers and many more results. In order to classify the data that produce those results a classification and rating mechanism will be defined from the NECOMA consortium before those results are transferred to the appropriate Policy Enforcement Points defined. This will be achieved by attempting to identify low-quality sources, rate their relevance to the observed data, and group the resources into different classes (e.g. CVEs, popular press, mentions & statistics).

IMPACT/MARKET INVOLVEMENT

NECOMA consortium has made a quite long list of meetings with the industry along with both active and planned collaborations. These actions aim for industry adoption of NECOMA results and also to augment the exploitation po-

Coordinator 1

Nara Institute of Science and Technology (JP)

Partners

Innovation Institute
National Institute of Informatics
Keio University
The University of Tokyo

Coordinator 2

Institut Mines-Telecom (FR)

Partners

Atos Spain S.A (ES)
Foundation for Research and Technology (GR)
Research and Academic Computer
Network NASK (PL)
6cure SAS (FR)

NECOMA



3 years
(01-06-2013 to 30-04-2016)



10 Partners



5 Countries



€ 1.459.000 EU Contribution

<http://www.necoma-project.eu>



¹ <https://github.com/CERT-Polska/n6sdk>

² http://www.necoma-project.eu/m/filer_public/b1/6f/b16f7d2e-391c-4571-b1c3-dced-bd1f5446/ut_tazaki_badgers2014.pdf

³ http://www.necoma-project.eu/m/filer_public/b8/47/b8475f20-0332-43ee-a35d-47e072cf1e0b/ijj_lorchat_badgers2014.pdf

tential for consortium members by obtaining early feedback from businesses, network operators and/or security vendors. Some of the organizations already contacted include Renater (FR), World Bank (US), ACDC (EU project), ACTIVE (JP), Telecom ISAC (JP). Moreover NECOMA industrial partners are actively exploiting the results as they are actively involved with DDoS mitigation techniques (6CURE as a DDoS mitigation vendor) and are major European players in the area of Cybersecurity (e.g. ATOS). Moreover, they are fully aware of the multi-layer approach against cyber-threats (IIJ) and are already involved in the process of designing and building a SDN based Programmable Internet Exchange in EDO (NAIST & UT).

PILOTS

NECOMA results will be demonstrated through four (4) main use cases. These include the DDoS mitigation scenario, the botnet introspection scenario, the smartphone user protection scenario and the malware campaign mitigation.

ZOOM IN

- The publications section of the site <http://www.necoma-project.eu/publications/>
- The deliverable D2.1 named "Threat Analysis" that provides an overview of the above research results.

New techniques to detect anomalies for mobile devices



NEMESYS

Enhanced Network Security for Seamless Service Provisioning in the Smart Mobile Ecosystem

«Some of the project's customers are our own industry and commercial partners. Since they are spending money on this project, they expect to get back and exploit for their own use the results that are being produced. So they are among our primary customers, including small and medium enterprises(SME) such as Hispasec. For a small company, they cannot be involved in the project unless they are going to actually put the results on the market. They have already started marketing the outputs of NEMESYS. Telecom Italia IT, with Telecom Italia are exploiting some of the results with Hispasec as well». **Erol Gelenbe, project coordinator**

The NEMESYS project addresses anomaly detection mechanisms for mobile devices, as well as the exploitation of detection for mitigation purposes as with signaling attacks. The project targets the identification of vulnerabilities in mobile devices and networks. **It designs novel tools such as honeypots to attract and detect anomalies.** NEMESYS works on approaches to detect and identify attacks against mobile users and against mobile networks that are run by the operators such as COSMOTE and Telecom Italia. We also investigate the nature of cyber threats in this area and provide tools, such as visual analytics to identify, classify and attribute threats and attacks.

RECENT DEVELOPMENTS

Among recent achievements of NEMESYS is the exploitation of state transitions in mobile devices that can be an indication of either malware or improperly designed applications. Thanks to this identification, an automatic technique to detect and mitigate attacks has been tested. The end-user might have applications installed willingly or insidiously (as part of an attack) on her mobile device that can make the device behave in ways which are unfavorable either to the user or the telecom operator, or both, e.g., consume an unreasonable amount of bandwidth, create unwarranted payment charges for the user, create needless congestion to the operator's bandwidth and signaling infrastructure, create distrust between the user and the operator, increase energy consumption for the mobile user device and/or the network operator, etc.. Another important result of the project is a software to be installed on mobile devices, which can capture state transitions or system calls in mobile devices that are indications of the presence of malware. A third useful output is a software that can be used by operator and large multi-user mobile customers (e.g. corporate clients) to visually track and attribute the security and attack status of the network.

The project has also developed the SECSIM simulation tool to simulate and mitigate against signaling attacks and DDoS attacks in mobile networks.

VALIDATION STRATEGY

The project has four use cases designed to evaluate and validate the delivered results:

- Mobile device protection against attacks;
- Detection of signaling based attacks against mobile networks;
- Anomaly detection for the femtocell architecture;
- Visual analytics for mobile network operators.


Coordinator

Imperial College London (UK)

Partners

CERTH (GR), COSMOTE (GR),
Hispasec (ES), Telecom Italia IT (IT),
Technical University of Berlin (DE)

NEMESYS

Call  3 Years
(2012-11-01 to 2015-10-31)


6 Partners


5 Countries


€ 2.750.000 EU Contribution

<http://www.nemesys-project.eu/nemesys/> 

HAVE A LOOK AT

- S. Liebergeld, L. Matthias and C. Mulliner, "No-madic Honeypots: A Novel Concept for Smart-phone Honeypots" in Proceedings of IEEE MoST 2013, that outlines the ideas of honeypot-based attack-detection approach of NEMESYS;
- Gokce Gorbil, Omer H. Abdelrahman, Mihajlo Pavloski, and Erol Gelenbe. Modeling and analysis of RRC-based signaling storms in 3G networks. IEEE Transactions on Emerging Topics in Computing, Special Issue on Emerging Topics in Cyber Security, PP(99):1–14, January 2015;
- Other papers on Network Security available online from <http://san.ee.ic.ac.uk>



OPTET

Operational Trustworthiness Enabling Technologies

Coordinator

Thales Communications&Security (FR)

Partners

SAP (DE), University of Duisburg-Essen (DE),
FORTH (EL), University of Southampton (UK),
ATC (EL), SINTEF (N), IBM (IL),
AMOSSYS (FR), Provicel (FR),
Thales Research and Technology (NL),
Athens University of Economics and Business (EL),
iMinds (BE), Brandenburg University
of Applied Sciences (DE), Thales Services (FR)

Internet users find out an increasing amount of stories of malware, spyware, hackers and security-holes every day; as a result they do not know who to trust or what is trustworthy anymore. The OPTET project aims to amend that situation and substantially increase the trust and confidence in Internet based systems, applications and services. To achieve this goal, OPTET considers socio-technical systems, identifies processes to manage the trustworthiness of these systems and develops technologies that enable evidence-based trustworthiness management. The results will be demonstrated and evaluated in the context of two operational use cases.

APPROACH

OPTET defines an unique approach that is designed to cover all relevant aspects of a software development and operation life cycle. The project has developed a unified cross-disciplinary model of trust and trustworthiness: designed by a team including social scientists, economists, legal experts & computer scientists. This model is used to represent and quantify the trust of all stakeholders and the trustworthiness of socio-technical systems.



The OPTET life cycle

THE OPTET LIFE CYCLE

The OPTET project will deliver a full life cycle approach, from design to deployment and monitoring of trustworthy systems based on evidence.

The project will deliver a unified model of trust and trustworthiness and a set of Generic Enablers that can be integrated into existing platforms to improve trust and trustworthiness in a holistic manner.

INNOVATION ACHIEVEMENTS

The main innovation achievements are the Generic Enablers offering:

- Capacity to design Trustworthy Socio-Technical systems, assisted by a trustworthy engineering process and capabilities including the identification of the threats that may compromise the system;
- Capacity to develop trustworthy applications and get them certified;
- Capacity to submit an application together with its certificate, enable decision making based on trustworthiness information;
- Capacity to detect and react to change in system's trustworthiness and/or user's trust with the overall objective to maintain it/those at a desired (satisfactory) level.

DEMONSTRATION AND EVALUATION

The project results will be integrated into two existing platforms (Fi-Ware and Docker), and demonstrated and evaluated in the context of use cases in two different domains: Cyber Crisis Management and Ambient Assisted Living.

IMPACT

The project will deliver a set of tools for trustworthy engineering. These different tools, depending on their maturity, will be presented in different events in order to make their promotion. The project aims to contribute in standards ISO 25000 series for adding trustworthiness.

OPTET	
Call 8	3 Years (2012-11-01 to 2015-10-31)
	15 Partners
	8 Countries
	€ 7.094.162 EU Contribution
	www.optet.eu

A secure data storage with biometrics sensors



PCAS

Personalised Centralized Authentication System

GOALS & STRATEGIES

Current mobile device users concerns related to confidentiality of the personal data they store on their smartphones are increasing. Users now store more information on their handheld devices, and use it as a regular computer installing applications without much concern on security and privacy of data. This new use for mobile devices increases risk and requires new data protection approaches: it has been demonstrated that many third-party applications try to collect as much information from the device as possible in order to send it to their servers.

Although, mobile devices are now equipped with robust protection mechanisms, secure hardware components and new software architectures, in order to tackle these new security risks, its use is still controlled and limited by the mobile operators.

PCAS aims at providing an innovative, trustworthy, handheld device: the Secured Personal Device (SPD). This novel device is a smartphone accessory that allows users to securely store their data, to share it with trusted applications, and to easily and securely authenticate him. Security is increased isolating the data from malicious applications on the smartphone.

The SPD will recognize its user using multiple biometric sensors, including a stress level sensor to detect coercion. Using the same biometric authentication, the SPD will be able to enforce secure communication with servers in the cloud, relieving the user from memorizing passwords.

INNOVATION ACHIEVEMENTS

PCAS will innovate on two different areas: development of novel security related techniques and creation of a new market.

With respect to security research and innovation, PCAS will:

- **Enhance smartphones security:** Using available secure hardware elements (eg ARM processors Trustzone), it will be possible to define novel software protection environments and programming tools. This will allow the hardening of existing software and to develop secure elements (interaction with the user, secure storage or communication);
- **Develop novel mobile biometric authentication mechanism:** The PCAS project will deliver novel algorithms using alternative sensors and algorithms: motion and director (used in air signatures), of hand palm recognition or hearth rate monitor (for coercion detection);
- **Integrate biometric authentication into the cloud:** The SPD will allow the user to authenticate on a smartphone using biometrics. The infrastructure provided by PCAS will allow to extend that authentication to remote services on the cloud. The system will use biometric information to identify the user, but guaranteeing that no biometric data leaves the SPD. After the identification the remote cloud service can use the provided identification to authenticate the remote user;

With respect to market-oriented innovations, the following are more relevant:

- **Implementation of a smartphone peripheral:** There are no products available in the market that extend smartphones with added functionality. With respect to the Google Android ecosystem, the OS level support to physically connect peripherals is limited. The PCAS project will

Coordinator

INESC ID (PT)

Partners

O.S. New Horizon-Personal Computing Solutions (IL)






Maxdata Informatica (PT)

Polytechnic University of Madrid (ES)

Norsk Regnesentral (NO)

AFCON Control&Automation (IL)

CEA-LETi (FR)

PCAS
 3 Years (01.10.2013 to 30.09.2016)
 7 Partners
 5 Countries
 € 3.249.250 EU Contribution
http://www.pcas-project.eu/ 



provide and make publicly available techniques and guidelines to allow the implementation and connection USB of devices to an Android smartphone.

- **New mobile secure storage mechanism:** The project will present a full featured Android smartphone peripheral providing a secure storage encrypted with key based on biometric information that will not leave the SPD. Being external, devices data access security is increased (since all accesses should be authorized by the user) and provides a security mechanism not managed by the smartphone constructors or mobile operators. The PSD will also allow then access of data on multiple devices to share information, or when replacing the smartphone.
- **Server-side infrastructure to allow secure data synchronization:** Although the SPD is a fundamental security element of the PCAS environment, the data stored in can be produced and delivered by a remote server. PCAS will provide an architecture of components that will connect the SPD and existing server. These components will allow the user authentication to remote services and secure upload of data to the SPD. During the project this architecture will be tested when integrating the SPD with already existing services;
- **Integrated development environment for the development of mobile secure applications:** The access of information will be mostly performed in the smartphone. To help developers, the PCAS project will provide a set of APIs and tools to ease the development of such applications. By building these tools the value of a SPD will increase greatly, since new secure services (locally on the smartphone) or remotely on cloud services) will be implemented.

PCAS will produce a complete ecosystem composed of the Hardware accessory, software mobiles (on the smartphone) and servers to allow the secure access/transfer of data, the infrastructure to allow service providers to adapt existing services to the PCAS concept.

OVERCOMING CONSTRAINTS OF THE MARKET

The mobile devices market is constantly evolving so it might be challenging to propose a technology that works with a high range of available devices. Furthermore most currently existing security mechanisms (e.g. ARM trust-zone) need implementation by the operating system vendor, but require the explicit activation by the mobile operator. For instance, Android systems already implements some security services, but due to operator decisions, those services may not be available to programmers or users

PCAS proposes a solution that is compatible with devices from different vendors (with minor mechanical adjustments) and with multiple operating systems (with a suitable middleware).

PCAS solution will also be free from operator lock-in, since it will be completely autonomous from the mobile operator and will use publicly available programming API.

MARKET OPPORTUNITIES

One of the target public of the PCAS concept are patients that have to store and manage large amounts of medical and clinical data. From the interviews to IT professionals on the Health area, standards and data protection laws are current obstacles to the implementation of a wide sharing of medical data using the usual data-center/cloud infrastructures.

With PCAS the medical information (that belongs to the patient) is carried with him, and presented to doctors. This removes any barriers to its sharing. The inclusion of a server side infrastructure in the project will allow the sharing of private information among several services providers. The private data will be owned and managed by the user allowing him to share it with several services providers (for instance multiple HMO).

Furthermore from the moment a secure element (not tied to any operator and with a public programming API) is available, new providers and services will emerge around the mobile phone.

MARKET INVOLVEMENT

The PCAS results will offer protection for sensitive data of citizens stored on their mobile devices. The application domain for PCAS is quite big: the secure add-on can evolve not only in secure storage, but also in a secure execution environment for mobile device.

Moreover, the healthcare domain has huge potential for application of mobile technologies – as confirmed recently by the move of Apple in this area with their new iOS release. The members of the project already got in touch with hospitals and several patient associations, that showed high interest towards the product. The public sectors and the public services will be then involved in the exploitation plans.

Since a support infrastructure targeted at the programming and implementation of addition services and applications will be publicly available. Several organizations will be able to extend their services or products to take advantages of the SPD.

With respect to the direct consumers targets PCAS envisions two large groups: regular citizens, willing to buy a device that guarantees secured data and personal access, and companies that already offer some service but what to innovate and increase the security of user authentication and data transfer (e.g. banks or HMO).

PCAS already include three industrial partners: a start-up that idealized the PCAS concept, a leader on clinic data management and a large software supplier and systems integrator. This diversity offers the project a wide and rich view of the problems and opportunities faced during and after the project.

Furthermore at the end of the project each one these partners can continue the project offering commercial goods of services.

PILOT

After the implementation of the hardware prototype and the software components, the validation planned by PCAS will be based on two use cases. One use case focuses on micropayment services and user authentication in a university campus scenario: students will be allowed to identify themselves with a smartphone and pay for services such as photocopies or coffees. The other use case,



that is heavily industry driven focuses on handling medical clinical exams data: it is led by MAXDATA (already producer of software for clinical exams companies) and will extend the already available cloud base infrastructure with the SPD.

We will develop a set of applications that will allow these exams to be shown on the user's smartphone or on the doctor's desktop computer, always in a secure manner. This can be an example of a personal health record that is automatically updated with the information from clinics or laboratories, a personal health record that can be carried and accessed by the user, and a personal health record that can be shown to others always with the authorization of the user and only of the user".

HAVE A LOOK AT

Please consult PCAS scientific papers already published:

- "Using ARM TrustZone to Build a Trusted Language Runtime for Mobile Applications" at the APLOS 2014 conference. <http://www.pcas-project.eu/index.php/publications/28-arm-trust-zone>
- "Low Computational Cost Multilayer Graph-based Segmentation Algorithms for Hand Recognition on Mobile Phones" at the The 48th Annual IEEE International Carnahan Conference on Security Technology. <https://www.pcas-project.eu/index.php/publications/29-low-computational-cost>
- "A comparative survey on Supervised Classifiers for Face Recognition" at The 48th Annual IEEE International Carnahan Conference on Security Technology. <https://www.pcas-project.eu/index.php/publications/30-comparative-face-recon>
- "Supervised classification methods applied to Keystroke Dynamics through Mobile Devices" at The 48th Annual IEEE International Carnahan Conference on Security Technology. <https://www.pcas-project.eu/index.php/publications/31-supervised-class-mobile>
- "Authentication Security through Diversity and Redundancy for Cloud Computing" at INForum 2014 | Portuguese informatics Symposium. <https://www.pcas-project.eu/index.php/publications/32-auth-redunt-cloud>



POSECCO

Policy and Security Configuration Management

Coordinator

SAP (DE)

Partners

University of Bergamo (IT),
Platte Consult (DE),
University of Innsbruck (A),
IBM Research (CH),
ATOS (ES),
Technical University of Eindhoven (NL),
Deloitte (FR),
Polytechnic University of Turin (IT),
Bern University of Applied Sciences (CH),
Thales Services (FR)

POSECCO

Call  3.25 Years
(2010-10-01 to 2013-12-31)


11 Partners


7 Countries


€ 6.999.987 EU Contribution

 <http://www.avantssar.eu>

OBJECTIVES

Internet service providers now have to manually resolve the inter-dependencies between high-level security requirements on one side and corresponding security policies and low-level configurations on the other side. In this, setting errors are inevitable due to high complexity of the systems and constant changes in requirements, policies regulations, and configurations. The PoSecCo project deals with this complexity by **establishing traceable and sustainable links between requirements and the configuration settings of appropriate security mechanisms in the system.**

INNOVATION ACHIEVEMENTS

The traceability link enabled by PoSecCo includes two key artifacts:

- The PoSecCo models represent both functional elements of IT systems at different abstraction levels as well as security-relevant information for each of these. The PoSecCo model repository can be further extended with new models suitable for different kinds of security policies;
- The PoSecCo integrated prototype smoothly consolidates different prototypes developed in the project. It includes 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.

MARKET ACCEPTANCE GAPS

An organization that wishes to adopt the PoSecCo technology has to invest into the production of security models for its own policies and functional elements.

MITIGATION STRATEGIES

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

PoSecCo also tries to improve acceptance by the end-consumers by investigating how to extend its model repository with other models used in industry, e.g. the data protection model.

IMPACT

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

ZOOM IN

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

sortium. The project has also identified performance indicators for the tools and is going to measure the prototype usage with respect to these key metrics.

The models are validated as a part of the tools; PoSecCo also tries to reach out to interested researchers and policy providers and get their feedback regarding the models.

As part of the project, **several patent applications have been filed by industry partners** of the consortium. Moreover, some of the tools developed have been prototypically integrated into products as to facilitate their future uptake.



Securing the cloud with cryptographic mechanisms

PRACTICE

Privacy-Preserving Computation in the Cloud

Coordinator
Technikon (AT)

Partners

University of Milan (IT),
Catholic University of Leuven (BE),
University of Bristol (UK),
Technical university of Eindhoven (NL),
Alexandra Institute (DK),
Aarhus University (DK),
Bar Ilan University (IL),
Georg-August University in Goettingen (DE),
INESC Porto (PT),
Technical University of Darmstadt (DE),
Cybernetica (EE),
Aerospace Technological District (IT),
Arcelik (TR),
Intel (DE),
SAP (DE),
Partisia (DK),
Julius-Maximilians University of Wuerzburg (DE)

PRACTICE

Call  3 Years
(01.11.2013 to 31.10.2016)



Partners



Countries



€ 8.424.029 EU Contribution



<http://www.practice-project.eu/>

Many organizations would like to use the benefits of cloud computing, but they do not trust the cloud service providers to store and process their data. Legal obligations, such as the data protection legislative might even prevent them. In this respect the secure multi-party computations and property-preserving encryptions are promising approaches that will allow enterprises to retain confidentiality and control of the sensitive information while storing and processing it in the cloud. The PRACTICE project comprises the leading experts in Europe in these domains, as **it sets out to develop a secure cloud framework equipped with the state-of-art cryptographic protocols for protecting the data.**

INNOVATION ACHIEVEMENTS

PRACTICE will deliver a secure cloud framework for enterprises that will include application development tools and secure computation protocols for protecting sensitive data and secure computations on these in the cloud.

OVERCOMING CONSTRAINTS OF THE MARKET

The secure multi-party computations technology and other cryptographic protection mechanisms researched by the project are already accepted on the market, but today most of these technologies are not yet mature enough to be an industry standard. In case of the lack of investment these technologies can lag behind its full potential and not reach the maturity soon enough. The project comprises several industrial partners, including big companies and startups, that see clear business applications for the future results and have customers asking for the tools PRACTICE develops. Regarding the Regulation, the project expects that it is moving into the right direction, because many people involved in it understand that technically encryption solves the privacy problem and the interpretation of the legislation is catching up.

USE CASES

The project plans to validate its results via a set of use cases and **two pilot studies**.

These include a **supply chain management scenario run by SAP**, which involves two project partners as end users: the Turkish consumer goods provider Arcelik and the Italian aerospace manufacturer Distretto Tecnologico. Furthermore, **a statistics use case is validated by the Danish start-up Partisia and the Estonian Cybernetica.**

MARKET INVOLVEMENT

Achievement of the project goals will bring the secure multi-party computations and other privacy-protecting technologies to the market, and will ensure that the EU stays the technology leader in this domain.

The main end-users identified in this initial period are corporations, large organizations and governments.

Risk assessment of large scale networked systems



RASSEN

Compositional Risk Assessment and Security Testing of Networked Systems

«Among other things, we demonstrate the benefits of the project by defining maturity levels for the areas that the project is addressing.

Progress for end-users in the project is measured by comparing their position on the maturity scales before and after the project. For instance, one of the areas we target is risk assessment.

The lowest level of the maturity scale is defined as risk assessment being performed informally, without any methods and tool support.

Higher maturity levels are defined as risk assessment being performed in a structured manner with method and tool support».

Fredrik Seehusen, project coordinator

The vision of RASSEN is to enable better communication and decision making related to cyber security. It takes the position that security should not be seen as a goal in itself, but a means of protecting one's assets. Therefore cyber security must be understood and reasoned about, not just at a technical level, but also taking into account the context in which software is used, organizational level assets, and legal issues. This requires vertical communication across the organizational hierarchy, involving people with different roles, backgrounds and experiences. The technical security experts are not necessarily those that assess the impact of organization level assets. The security managers are not necessarily those that make high-level decisions. The different roles have different requirements to the information basis on which to make a decision, both with respect to level of detail and focus. The further up we go on the organizational hierarchy, the less technical we need to be, and the focus is shifted to impact on legal issues and organizational assets.

Three innovations that are developed in RASSEN are:

- The RASSEN method for risk based security and legal compliance. This method combines three areas that are traditionally addressed in isolation: security risk assessment, security testing, and legal compliance. Concrete and practical guidelines for each step of the method are provided;
- The RACOMAT tool for component- and risk-based testing. This is a standalone tool which is under development in RASSEN which combines security testing and low-level component based risk assessment;
- The Smartesting CertifyIt extension for risk-based security testing. CertifyIt is a model-based testing tool which is being extended towards risk-based security testing within the RASSEN project.

RECENT DEVELOPMENTS

RASSEN has delivered the intermediate versions of the RASSEN method and toolbox. This includes new versions of the CORAS tool for risk assessment and the RACOMAT tool for component based risk assessment. It also includes guidelines for schematically generating risk models from a dictionary of attack patterns (CAPEC) and from legal compliance requirements.

VALIDATION STRATEGY

The project works with end-users in the financial, e-Health and IT domains to validate its results. RASSEN evaluates perceived usefulness and perceived ease of use for their technologies and tools, as well as the exploitation potential. The RASSEN innovations are also evaluated using a lean canvas approach.

Coordinator
SINTEF (NO)

Partners
Smartesting (FR)
FOCUS of Fraunhofer (DE)
EVRY (NO)
Software AG (DE)
University of Oslo (NO)
Info World (RO)

RASSEN

Call  8 **3 Years**
(2012-10-01 to 2015-09-30);


7 Partners


4 Countries


€ 3.069.335 EU Contribution

<http://www.rassen-project.eu> 



SWEPT

Websites through malware dEtECTION and attack Prevention Technologies

Coordinator

TECNALIA (ES)

Partners

EUROHELP Consulting SL (ES)

Montimage EURL (FR)

Everis Aerospacial y defensa SL (ES)

IVARX LIMITED (CYBERDEFCON) (UK)

Emaze networks SPA (IT)

S21Sec Information security labs SL (ES)

AMIS družba za telekomunikacije D.O.O. (SL)

CSIS security group AS (DK)

ARSYS Internet S.L. (ES)

ARIMA software design S.L.L. (ES)

SWEPT

Call CIP 3 Years
(from 01/03/2014 to 28/02/2017)

11 Partners

6 Countries

€ 1.993.000 EU Contribution

<http://www.swept.eu/>

PROJECT OBJECTIVES

The main objective of SWEPT project is to contribute to increase the trustworthiness of the internet by significantly improving the protection of websites against cyber-attacks, as well as the capabilities for the detection and mitigation of new attacks and the detection of already infected websites.

The SWEPT project proposes an innovative approach that combines and integrates concepts and solutions that come from previous academic research, open-source initiatives and the cybersecurity industry.

The proposed SWEPT security solution will combine preventive and detecting security mechanisms easy to adopt for maximizing website protection against malware and attacks.

INNOVATION ACHIEVEMENTS

SWEPT proposes a security solution that incorporates different security mechanisms and tools for automatically mitigating web site attacks, and thereby maximizing the security posture of websites with a minimum of intervention from web site owners and administrators. The proposed solution offers:

- A set of innovative preventive security solutions based on the "security by design" concept to be applied at the web application level for website protection (prevention of infections and avoidance of attacks), and that avoid the overhead and implantation difficulties generated by traditional external application firewalls. The technologies used in the preventive solution are based on HDIV open-source project.
- A set of more complementary detection security solutions to be applied externally to the web application level.
- A new security certification scheme based on the different technologies being proposed by the project.

All these services will be provided via a unique portal which will offer integrated both preventive and detective services.

IMPACT/MARKET INVOLVEMENT

The main beneficiaries of SWEPT platform will be website administrators and owners that will take advantage in a number of ways:

- The concept of security-by-design which it is centered on designing software systems that are secure from the ground up, minimizing the impact of a system breach when security vulnerability is discovered.
- Ensuring greater availability of the websites.
- A better understanding of the present vulnerabilities.
- The benefits of improving the cyber-crime fighting capacity and capability will have many long-term benefits for businesses and their customers, which come from the increase in customer trust and consumer confidence.
- Boosting economic activity through increased trust on web sites.

PILOTS

In order to demonstrate the feasibility and effectiveness of the proposed solution, the SWEPT project is planning for year 2016 the implementation of two business-oriented pilots:

- SWEPT Business Pilot 1: Service Pilot oriented towards website administrators and owners, Hosting service providers and Internet Service Providers.

This pilot will be focused on the application of SWEPT technologies and services to already developed websites by the different end users usually involved in a typical website operation scenario. The pilot targets to involve a very significant number of real web applications that run in real life scenarios. The pilot will evaluate the effectiveness of the applied both proactive (prevention of attacks) and reactive measures (detection of malware and vulnerabilities) as well as the usability of the tools.

- SWEPT Business Pilot 2: SWEPT Developer Service Pilot for website, web systems and backend developers. This pilot will demonstrate the applicability of the developed proactive prevention security measures by web designers and developers in a real life web application development scenario. The pilot will evaluate the effectiveness of the applied reactive measures (detection of malware and vulnerabilities) as well as the usability of the tools.

HAVE A LOOK AT

<http://hdiv.org/> open-source project as the principal foundation for the information flow control mechanisms proposed by the project in preventive measures.



Secure edge devices
to increase trust

TRESCCA

TRustworthy Embedded systems for Secure Cloud Computing Applications

Coordinator

OFFis (DE)

Partners

CoSynth (DE)

Wellness Telecom (ES)

vOSYS (FR)

Technological Educational institute of Crete (Gr)

ST Microelectronics (FR)

Telecom ParisTech (FR)

TRESCCA

Call  3 Years
(2012-10-01 to 2015-09-30)



7 Partners



4 Countries



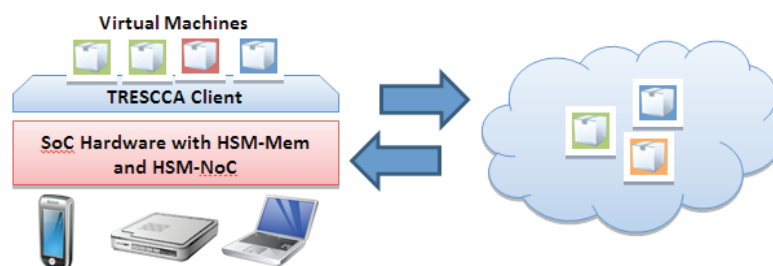
€ 2.950.000 EU Contribution



<http://www.trescca.eu>

OBJECTIVES

TRESCCA develops hardware and software technologies that improve the security of cloud edge devices. Secure cloud edge devices increase the level of trust of service providers towards end-users, and vice-versa. The project enables applications where **private data does not need to be transferred to the cloud but is only accessed locally by certified and trusted software.**



TRESCCA Platform overview

Hardware security in TRESCCA is realized through two key hardware technologies: an **on-chip component** that protects the external memory bus against sniffing attacks through cryptographic methods; and a **firewall-like extension for Network-on-Chips** enabling protection and isolation of virtual machines sharing multiple hardware components of a System-on-Chip. The fine-grained definition of access rights enables the realization of multiple isolated virtual compartments with different levels of security on one chip. Software security is realized through two key technologies: a hypervisor for ARM processors utilizing state-of-the-art and future hardware security



Migration of lightweight VMs between trusted devices and the cloud

technologies including the technologies developed by TRESCCA, which significantly improves the isolation between virtual machines and enables the co-hosting of application with different levels of trust on the same execution platform; and a framework and runtime environment enabling the migration of lightweight Virtual Machines between cloud servers and client devices. The basic idea behind this approach is to “move the application to the data” if the data is sensitive and should not leave the device.

RECENT DEVELOPMENTS

The project has developed first prototypes of the HW and SW security components during its second year:

- Initial versions of the memory encryption component and the Network-on-Chip firewall running on a FPGA/System-on-Chip development platform;
- A proof-of-concept implementation of the GlobalPlatform Trusted Execution Environment based on KVM-on-ARM hypervisor enabling strong separation and security between trusted and untrusted applications;
- Migration of VMs between an OpenStack cluster and the secure edge device. Due to the support of hybrid migration ARM-based VMs can also be executed on x86 server hardware.

The project has also started its integration and evaluation activities. All components will be integrated into a common System-on-Chip/FPGA prototyping platform. The applications that will be used for final evaluation are currently under development.

VALIDATION STRATEGY

The results of TRESCCA will be validated by developing an FPGA-based prototype of the client platform (integrating TRESCCA hardware and software components).

The following setups and components will be used for evaluation and validation of the results:

- Several cloud servers providing IaaS (Infrastructure-as-a-Service) using OpenStack and CloudStack. Servers are hosted and operated by several project partners;
- **A prototype of the TRESCCA client platform based on an FPGA-prototype board**, integrating all hardware and software components developed in TRESCCA;
- Three scenarios realized as different applications making use of the security features available on the cloud and client sides.

Scenarios will be partially implemented using a combination of emulated environment and proof-of-concept applications.

- **Smart Meter Gateway** – Protecting smart meter data against hardware and software manipulation and data leakage;
- **DRM** – Protecting copyrighted and protected content against manipulation and privacy with flexible control and management of access rights;
- **Secure authentication, verification and transaction of private data** – Protecting private data on client devices (addresses, banking data, passwords, key files) against data leakage, while allowing verification of private data only on client devices, so that private information does not have to leave client device, and there is no need to store (unencrypted) data on cloud servers.

Evaluation will be done by industrial partners including semiconductor companies, embedded and mobile solutions providers and cloud service providers.

EXPECTED IMPACT/INNOVATION

The TRESCCA platform will offer a solution for trustworthy cloud computing that provides privacy and trust for both the user and the service provider. Its trustworthy client extends the cloud into companies and private homes and at the same time provides a trusted zone for the handling of private data. The

level of trust and security that will be realized goes far beyond existing solutions which are either proprietary hardware solutions limited to specific architectures (ARM TrustZone, Intel TXT) or just software-based solutions susceptible to a whole range of software based attacks.

TRESCCA plans to contribute to the European standardization of a trustworthy cloud platform by providing access to its developed technology and solutions and by cooperating with existing standardization bodies and organizations, e.g. GlobalPlatform. Most of its results, including the memory encryption technology, will be available as open-source. While the results of TRESCCA will not directly lead to stand-alone end-user products its technology is expected to be integrated into several future cloud-connected products, such as smartphones, tablet PCs, set-top boxes, and the whole range of Internet-of-Things applications. The level of security and trustworthiness of these devices will be significantly increased.

HAVE A LOOK AT

Find out more information about the TRESCCA platform:

- Specification and Requirements for the TRESCCA Platform – available here: <http://www.trescca.eu/downloads/D1.2.pdf>.
- A virtual prototype (software model) and initial software driver of the memory bus encryption module are available for download on <https://sec-bus.telecomparistech.fr>.
- All related software for VM migration prototype between Clouds and local clients available at Github: <https://github.com/trescca>.
- Code for Hybrid Migration enabling HW-accelerated ARM-VMs to continue their execution on x86 hosts: <https://git.virtualopensystems.com/trescca/qemu>.



A new methodology to model cyber security

TRESPASS

Technology-supported Risk Estimation by Predictive Assessment of Socio-technical Security

Coordinator

University of Twente (NL)

Partners

Technical University of Denmark (DK),
Cybernetica (EE), GMvIS SKYSOFT (PT)
GMv SGI (ES), Royal Holloway, University
of London (UK),itrust Consulting (LU)
Goethe University Frankfurt (DE), IBM Research (CH)
Delft University of Technology (NL)
Hamburg University of Technology (DE)
University of Luxemburg (LU)
Aalborg University (DK), Consult Hyperion (UK)
BizzDesign (NL), Deloitte (NL)
LuST (NL)

The TRESsPASS project works on providing decision support systems for cyber security investments in the socio-technical context, thus **taking into account not only IT infrastructure threats, but also threats related to the human behaviour like social engineering.**

The project works 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.

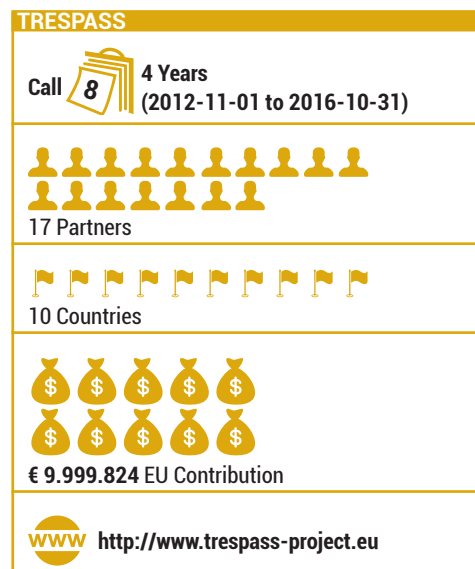
There is excellent opportunity for exploitation of the results, and the coordinator has experience with successful spin-offs: «*At the University of Twente we have a spin-off that's called Security Matters. There was a series of national projects that formed the basis of this. From my point of view as a coordinator, that would be definitely a success story*» said Wolter Pieters.

RECENT DEVELOPMENTS

TRESsPASS has developed an **approach for plugging in attacker profiles to support automated analysis of the system with various attacker profiles** – from script kiddies to experienced hacker organizations and targeted attacks. The project also works on **different approaches to attack visualisation that could assist security professionals and stakeholders in taking decisions.** The range of the visualisation techniques used in the project varies from formal models (e.g., attack trees) to physical models of the LEGO environment.

VALIDATION STRATEGY

The project includes **three case studies in the domains of cloud computing infrastructure** (IBM Research in Zurich), **telecom infrastructure** (Goethe University in Frankfurt) and **IPTV payment systems** (Consult Hyperion in UK). For the telecom infrastructure case study the focus is on detecting fraud with telecom services, while for the IPTV the main goal is to ensure customer privacy protection when dealing with sensitive financial services for IPTV.



HAVE A LOOK AT

TRESsPASS builds a community of socio-technical security professionals through a sequence of workshops. The next edition will be co-located with CSF in Verona in July 2015: <http://www.gramsec.uni.lu/>. TRESsPASS will also host the New Security Paradigms Workshop (NSPW) in Twente in September 2015: <http://www.nspw.org/2015/>. A visualisation workshops is planned at the 2015 CSP Forum.



UTRUSTIT

Usable TRUST in the Internet of Things



The uTRUSTit project focuses on the understanding of user trust in the Internet of Things and on the development of means to increase trust. Interconnected sensors, devices and objects can help us to improve our everyday life in a variety of areas (e.g. being healthy, being more productive etc.). However, it is very difficult to understand the underlying implications on information security and privacy that come with the Internet of Things. **uTRUSTit aimed at exploring factors affecting user trust and translating these factors into highly effective interface paradigms and approaches.** These paradigms were realized in form of accessible prototypes and a rule-based Trust Feedback Toolkit visualized by the security advisor, informing users about risks, security and possible consequences of their actions. uTRUSTit iteratively validated this

knowledge applied to **three use cases: a smart home, a smart office and an eVoting use case.** Several evaluations and field trials, also using Virtual Reality to simulate the Internet of Things environments have been conducted. Furthermore, uTRUSTit provided policy recommendations regarding legal aspects of data processing and transparency in the Internet of Things.

INNOVATION ACHIEVEMENTS

uTRUSTit provides the following key results:

- The Trust Feedback Toolkit – a rule-based API providing the user with information about Internet of Things system security and consequences about possible user actions. The feedback provided by the TFT is visualized by the security assistant;
- An in-depth understanding on factors that affect user trust and innovative and valid methods to assess user trust (e.g. with questionnaires and physiological measurements);
- User interaction and interface paradigms and approaches to increase user trust in the Internet of Things which are summarized in design guidelines;
- Knowledge about the applicability of these paradigms and approaches in smart home, smart office and eVoting use cases;
- A Virtual Reality simulation and evaluation environment to simulate Internet of Things settings and device interaction and natural movements as part of user evaluations;
- A set of accessible demonstrators showcasing security critical Internet of Things interaction in the three scenarios: smart home, smart office and eVoting- Policy recommendations on legal aspects of data processing and transparency in the European Union

Coordinator
CURE (AT)

Partners
Sweden Connectivity (SE)
Search-Lab (HU)
Technical University of Chemnitz (DE)
Norsk Regnesentral (NO)
Catholic University of Leuven (BE)

UTRUSTIT

Call 5 3 Years
(2010-09-01 to 2013-12-31)

6 Partners

6 Countries

€ 2.399.506 EU Contribution

<http://www.acdc-project.eu>

MARKET ACCEPTANCE GAPS

All developers, providers and suppliers in the Internet of Things domain can benefit from uTRUSTit project results. The results (e.g. the Trust Feedback Toolkit) can be integrated in a variety of applications, technologies and services. For the project results to be adopted, according changes in the user interface and user interaction flows have to be made in these applications, technologies and services.



MITIGATION STRATEGIES

Although the project has ended, uTRUSTit currently seeks exploitation possibilities and actively networks with industry and related research projects (e.g. ANI-KETOS and TWISNET).

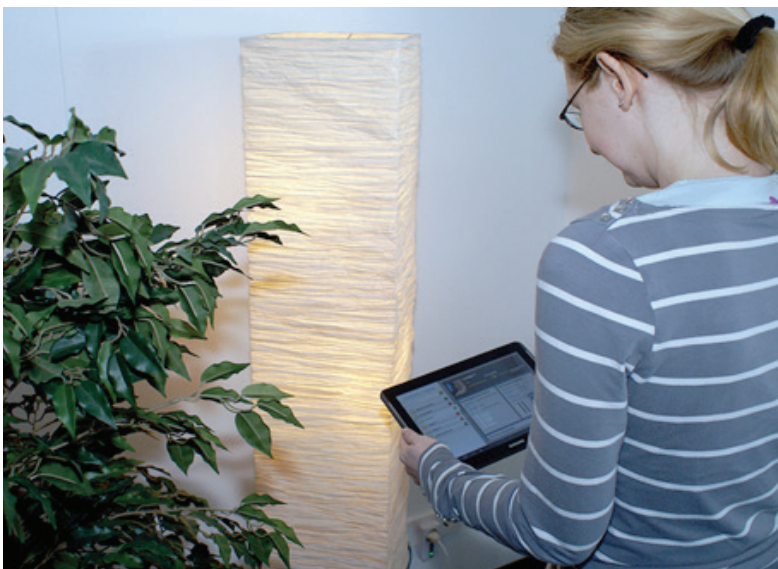
IMPACT

Availability of the results of uTRUSTit will enable a better user experience for Internet of Things infrastructures and will therefore result in a higher uptake and adoption of products and

services in the Internet of Things. This can lead to higher revenue for companies that sell these products and services. Perceived trust of end-users, created by information about privacy and security, is seen as one of the key factors in the success of the future IoT. The concepts of advanced interaction and user interfaces to provide trustworthiness feedback, the uTRUSTit TFT architecture and according hardware developed in uTRUSTit can be used as the much needed starting point for creating and developing future trusted and trustworthy IoT systems.

ZOOM IN

The project has run three use cases: smart home, smart office and eVoting. Over the course of the project more than 100 end-users took part in the validation activities, with their feedback continuously feeding into the prototype design and implementation.



HAVE A LOOK AT

YouTube-Channel: <https://www.youtube.com/user/uTRUSTitStudios>



VIS-SENSE

Visual Analytic Representation of Large Datasets for Enhancing Network Security

The goal of the VIS-SENSE project, funded by Call 5, was the research and development of **novel technologies for the identification and prediction of complex patterns of abnormal behaviour in network security domain**. The project aimed to combine the mining and analysis of large amounts of heterogeneous data with novel interaction and information visualisation technologies. The ultimate goal was the **enhancement of international network security through the stimulation of proactive measures** that would increase the effectiveness of analysis attempting to prevent or resolve cyber-crime.

These technologies were focused on **two scenarios: Visual Analytics of the Internet Threat Landscape and the Visual Analytics of Attacks Against the Control Plane** (BGP - Border Gateway Protocol). The objective of the first application scenario was to make security monitoring more effective for both known and unknown threats. It was focused on security investigations and root cause analysis using data-mining and visualization technologies on very large security data sets (which included as input spam data, scam and phishing emails, malware samples, and client-side threats targeting Internet user). The second application scenario aimed at collecting and analysing data about the state of the Internet routing infrastructure and to correlate them with other sources of information related to attacks targeting end hosts.

A number of target groups were identified, for which the project results would be relevant: **telecommunications operators and ISPs** would be interested in developments addressing BGP hijacks and attack attribution; **software security companies and businesses** would benefit from the VIS-SENSE project results by incorporating the next generation of tools into their security management consoles. **CERTs (Computer Emergency Response Teams)** could incorporate into their arsenal of monitoring tools some of the new VIS-SENSE technologies. These would enable them to respond more effectively to security incidents but also to remain informed of changes or evolutions in attack phenomena occurring in the networks that they are monitoring. Lastly, the general public should see the results of VIS-SENSE and its potential for improving the protection provided by security vendors.

The project has resulted in the **development of 16 high-quality, exploitable software artefacts**. These range from new data collection infrastructure to analytics modules and visualization components. A number of the visualization components have been integrated into the VIS-SENSE website for dissemination purposes. In addition, a visual analytics framework was created with the goal of integrating these heterogeneous components into a single visual analytics system for network analytics.

A total of 25 successful scientific publications were achieved during the project. The publications have proven the scientific value of the software developed within the project and have shown its utility in the solution of relevant problems within the network analytics domain.

In particular, project partners were able to identify and confirm instances of fly-by spamming; short-term IP prefix hijacking for malicious purposes. Instances of BGP-hijacking identified on the control plane (BGP) were successfully correlated with spam sent in the data plane (IP). The spam was also shown to belong to cohesive campaigns. Thus, a primary and ambitious objective of the project was successfully achieved.

Coordinator

IGD at Fraunhofer (DE)

Partners

Telecom SudParis (FR)

CERTH (GR)

University of Konstanz (DE)

Symantec (IE)

EURECOM (FR)

VIS-SENSE

Call 5 3 Years
(2010-10-01 to 2013-09-30)

6 Partners

4 Countries

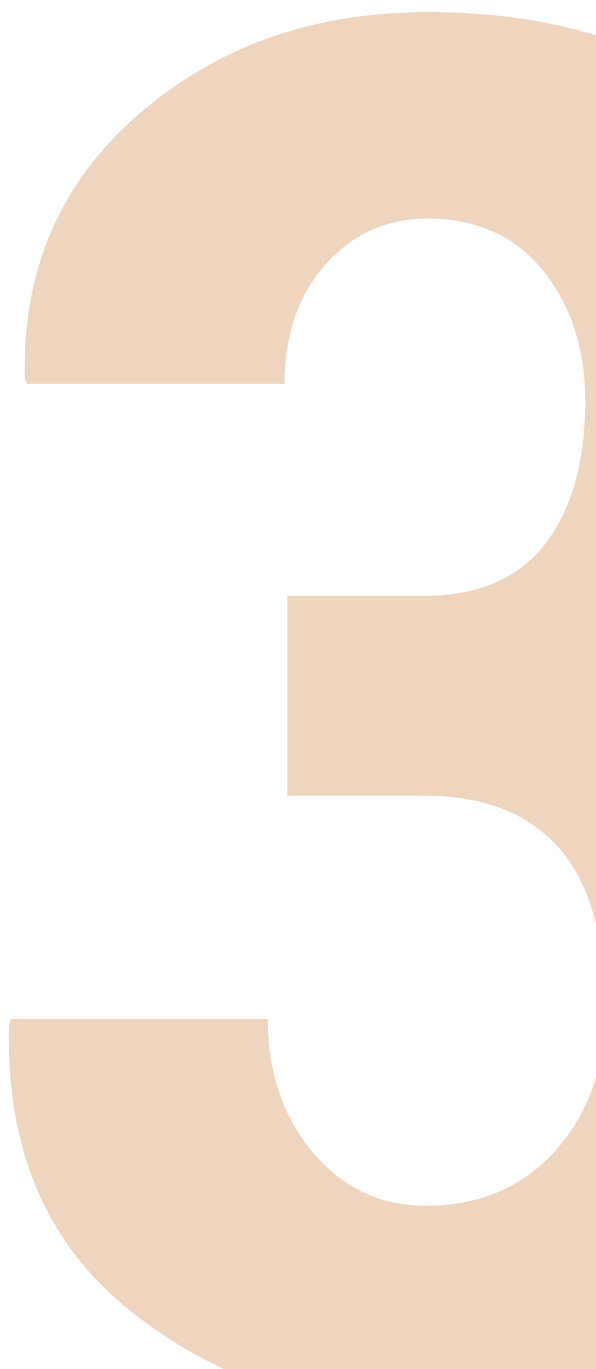
€ 2.350.000 EU Contribution

<http://www.vis-sense.eu>

Dissemination played an important role throughout the project. Partners participated actively in clustering activities, as well as dissemination activities in academia and industry. A direct result of these activities was a series of collaborations, in which VIS-SENSE prototypes were reused in the analysis of external data. These collaborations have continued beyond the end of the project. Finally, efforts in the active exploitation of the VIS-SENSE results continue. **Fraunhofer IGD is pursuing on a licensing model and funding sources for an open source release of the VIS-SENSE framework. Technology-transfer activities have occurred within Symantec and are being pursued by both CERTH and the University of Konstanz.**

3

TECHNICAL PROJECTS





A set of tools for different actors in the cloud

A4CLOUD

Accountability For Cloud and Other Future Internet Services

Coordinator

HP (UK)

Partners

Athens Technology Centre (Gr)
Cloud Security Alliance Europe (uK)
ARMINES (FR)
EURECOM (FR)
Furtwangen University (DE)
Karlstad University (SE)
Queen Mary University of London (UK)
SAP (DE)
University of Malaga (ES)
SINTEF (NO)
Tilburg University (NL)
University of Stavanger (NO)

«Imagine I am a CEO of a medium-sized company, and I want to produce a cloud service. I understand that it's better for me, for my value propositions to my customers, for dealing with regulations. And if I want to be accountable, what does it mean? I need a recipe book, I need to worry about processes and practices. Within my team I might need to deploy some functions to monitor accountability, and then I need to put some processes and practices in place to do that, and some tools to support that». **Nick Wainwright, project coordinator.**

A4CLOUD focuses on accountability for managing user data in the cloud. The project works on a set of tools for different actors in cloud: users, providers and those involved in regulation and governance. At the same time **A4CLOUD produces architectural practices and processes for cloud service producers and providers and the users of data in cloud services.** The project also develops a conceptual framework for accountability, identifying what does it mean to be accountable in the cloud.

A4cloud

Call  3,5 Years
(2012-10-01 to 2016-03-31);


13 Partners


8 Countries


€ 10.000.000 EU Contribution

 <http://www.a4cloud.eu>

RECENT DEVELOPMENTS

The project has developed the conceptual framework for accountability (<http://www.a4cloud.eu/contactus>). **The main accountability attributes identified by A4CLOUD are: transparency, responsibility, remediability, liability, observability, verifiability and attributability.** Currently A4CLOUD focuses on defining the use cases before transitioning into the second phase of the project – the architecture design and the demonstrator development.

"We have taken the conceptual framework for accountability, which is a very long deliverable, and we bashed it down into a short 20 page paper that should be consumable by people. We have created a project that works for organizations, we want to make organizations to think about becoming accountable" Nick Wainwright.

VALIDATION STRATEGY

Three main use cases are considered in the project. One use case focuses on an example of **an individual cloud, where a citizen can receive soft health-care services.** The main aspect in this use case is dealing with the personal information of the individual. The second use case deals with a **business-related cloud service**, where the focus is on a retail company that brings in location-based services for customized marketing. The third use case deals with **multi-tenanted cloud services.**

HAVE A LOOK AT

Deliverable D35.1 Metrics for Accountability reports on metrics for measuring accountability of cloud services based on the conceptual framework attributes. The deliverable reviews the attributes definitions and identifies how these can be measured.



ANIKETOS

Secure and Trustworthy Composite Services

OBJECTIVES

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

INNOVATION ACHIEVEMENTS

ANIKETOS worked on the following innovative artefacts:

- A language to express security and trustworthiness requirements on socio-technical systems: **the Socio-Technical Security Modelling Language (STS-ml) and the accompanying tool (STS-tool).**
- The security-by-contract paradigm for services that enables services to express their security and trust requirements in their machine-readable contracts.

The ANIKETOS platform and accompanying tools support service designers in building composite services that meet security requirements, and system administrators to monitor execution of composite services and react in case of violations.

MARKET ACCEPTANCE GAPS

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

MITIGATION STRATEGY

ANIKETOS actively disseminated its results to potential stakeholders.

Most of the results from the project are available as Open Source. These are found on GitHub at github.com/AniketosEU.

IMPACT

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

ZOOM IN

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

Coordinator

SINTEF (N)

Partners

ATOS (ES), Athens Technology Center (GR), DAEM (GR), DeepBlue (IT), SELEX (IT), CNR (IT), Italtel (IT), Liverpool John Moores University (UK), SAP (DE), SEARCH-LAB (HU), Tecnia (ES), Thales (FR), Waterford Institute of Technology (IE), University of Trento (IT), WIND (IT), ICT&S Center at University of Salzburg (AT)

ANIKETOS

Call 5 3,5 Years
(2010-08-01 to 2014-05-31)

17 Partners

10 Countries

€ 9.600.000 EU Contribution

<http://www.aniketos.eu>

HAVE A LOOK AT

See the promotional video on the project web site www.aniketos.eu, check out the newsletters and download the deliverables.

Open Source results are found at github.com/AniketosEU.

Discover more details of the Security Requirements modelling tool at www.sts-tool.eu



ASSERT4SOA

Advanced Security Service cERTificate for SOA

Coordinator

SAP (DE)

Partners

University of Milan (IT)

The City University (UK)

ENGINEERING (IT)

University of Malaga (ES)

Ugo Bordonni Foundation (IT)

SIT at Fraunhofer (DE)

ASSERT4SOA

Call  3 Years
(2010-10-01 to 2013-09-30)



7 Partners



4 Countries



€ 3.400.000 EU Contribution



<http://www.assert4soa.eu>

OBJECTIVES

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

INNOVATION ACHIEVEMENTS

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

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

MARKET ACCEPTANCE GAPS

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

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

MITIGATION STRATEGIES

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

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

IMPACT

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



ZOOM IN

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

HAVE A LOOK AT

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



COMIFIN

Communication middleware for monitoring financial CI

Coordinator

Elsag Datamat (now Selex Elsag) (IT)

Partners

Technical University of Darmstadt (DE)

IBM (IL)

Waterford Institute of Technology (IE)

Ministry of Economics and Finance of Italy (IT)


OptXware (HU)

KreditTilsynet (NO)

University of Modena (IT)

CINI (IT)

COMIFIN

Call  3 Years
(2008-01-01 to 2010-12-31)



9 Partners



6 Countries



€ 2.350.000 EU Contribution



<http://www.comifin.eu>

GOALS & STRATEGIES

As remarked in very recent studies of the Federal Reserve (<http://www.federalreserve.gov/>), a financial infrastructure is an unmanaged large scale networked system of interconnected financial markets and banking systems by which domestic and international financial institutions allocate capital and manage their risk exposures. **The 9/11 attack and European and North American black-outs over the past decade have emphasized vulnerability of this infrastructure to wide-scale disruptions and highlighted inter-dependencies between the financial infrastructure and other critical ones** (notably the power grid, telecommunication infrastructure and the Internet).

Nowadays ICT-based financial infrastructures are becoming largely used by financial actors, businesses, and ordinary people worldwide in order to carry out everyday financial activities. As a consequence, a large amount of financial transactions are being conducted over such ICT financial infrastructures, generating traffic that is carried also over publicly accessible communication mediums (for example, Internet), and involves commodity hardware and software. In order to guarantee key requirements such as stability, availability, and continuity of the financial services, **it becomes crucial to protect the above mentioned infrastructures from faults and security attacks that may significantly compromise the result of financial transactions**. As of today, attempts to guarantee such a protection are investigated on an intra financial domain basis only (such as inside a bank or a brokerage firm), ignoring those threats that can arise from cross domain interactions. Cross-domain interactions may span different organization boundaries as they may involve a variety of infrastructure systems such as telecommunication supply, electricity supply, banking, insurance, and finance agencies. We call the set of these systems the *global financial ecosystem*.

The emerging trend towards globally integrated enterprises raises a urgent need of monitoring the overall financial ecosystem in order to improve the situation-awareness of each involved organization. This advanced form of global monitoring is currently missing. CoMiFin aims to enhance the situation-awareness of financial organizations with the use of a distributed and secure monitoring software system. The CoMiFin middleware system enables financial institutions (and other critical service providers) to share information and resources for the purpose of identifying globally scoped attacks and threats against their IT infrastructure and business.

The main purpose of the CoMiFin STREP is strategically targeting improvements of the EU technological and institutional pace in addressing financial infrastructure protection (FIP).

Specifically, CoMiFin aims to provide "an infrastructure level monitoring, notification and mitigation" middleware as an essential element of FIP. CoMiFin aims at supporting business continuity of a financial actor on top of an unmanaged network of managed financial infrastructures under all foreseeable failure scenarios including the operational failures and deliberate breaches. To ensure that the technology developed by CoMiFin fits well into the overall holistic approach behind FIP, we will leverage the expertise of both: prominent user partners present in the consortium and Financial User Advisory Board members alongside the technological partners.

Addressing concerns about cloud service security



CUMULUS

Certification infrastrUcture for MUlti-Layer cloUd Services

«Cloud privacy and security are becoming urgent matters since the advantages from the economic and management points of view are driving companies and organizations to adopt cloud computing before it is secure enough. Approaches for security, privacy and quality-by-design must be encouraged and widely adopted if we want to have reasonably secure cloud services and, more widely, ICT systems». **Bartolomeo Sapio, project coordinator**

The CUMULUS project addresses cloud security issues by developing a **novel infrastructure for certification of multi-layer cloud services**. The infrastructure provides models, processes and tools to support certification of compliance with security properties for all types of cloud services, including infrastructure (IaaS), platform (PaaS) and software services (SaaS). The main instruments for ensuring service trustworthiness will be testing, monitoring and Trusted Computing proofs and their combination. The preliminary results includes all three basic types of certification models and mechanisms, cloud certification and identification of security requirements in the cloud infrastructure. **A security-aware Service Level Agreement (SLA) specification language**, the CUMULUS framework architecture and the associated engineering process, **is being developed**. The contribution is already a significant progress compared to the state of the art.

INNOVATION ACHIEVEMENTS

CUMULUS works on the following technologies and tools:

- An integrated security certification framework able to orchestrate the use of security-asserting tools;
- New automated and evidence-based models and processes for certifying security of cloud services;
- New tools for testing, monitoring and Trusted Computing proofs to support certifications;
- Processes and tools to support the usage of cloud service security certificates;
- Design systems relying on these certificates.

OVERCOMING CONSTRAINTS OF THE MARKET

The cost/benefit tradeoff for the CUMULUS results usage might not be clear for organizations in markets with no regulatory requirements for certification. In order to stress the importance of the standardisation of certification processes for cloud services, CUMULUS partners participate in several international initiatives and work on the open certification framework and the STAR registry of Cloud Security Alliance. CUMULUS results have a high potential to influence upcoming standards in the field of secure cloud and Trusted Computing (such as NIST RATax metrics, EU C-SIG, ISO 19086, CWA RACS, TCG TPM).

MARKET INVOLVEMENT


The CUMULUS achievements will become enabling technologies for building user trust in the cloud computing by providing reliable certification mecha

Coordinator

Ugo Bordonì Foundation (IT)

Partners

Wellness Telecom (ES)
The City University (UK)
University of Milan (IT)
Infineon Technologies (DE)
University of Malaga (ES)
ATOS (ES)
Cloud Security Alliance Europe (UK)

CUMULUS	
Call  8	3 Years (2012-10-01 to 2015-09-30)
 8 Partners	
 4 Countries	
 € 2.845.974 EU Contribution	
http://www.cumulus-project.eu 	



nisms for security. CUMULUS results have been grouped into ten individual exploitable items and corresponding exploitation strategies have been defined using business Canvas models. Potential users and stakeholders have been approached via advisory board workshops and via a questionnaire on different technical and business aspects related to CUMULUS. The answers give valuable and concrete hints for further development.

PILOTS

The project plans involve **two industrial scenarios** for requirements gathering and for validation and evaluation of the outcomes: **E-Health (together with ATOS) and Smart Lighting (Wellness Telecom is involved)**. The CUMULUS certification mechanisms are applied to both scenarios and a number of security properties is going to be certified in the pilot scenarios.

Security assurance for critical systems early in the life cycle



D-MILS

Distributed MILS for Dependable Information and Communication Infrastructures

Today's critical IT systems can be responsible for very sensitive operations, and the costs of a security failure in such a system can be extremely high. Therefore, it is widely acknowledged that critical systems must undergo a rigorous security assurance process that should start at the design stage of the life cycle.

However there is little automated tool support for early security assurance in critical distributed systems. The Distributed MILS (D-MILS) project provides technology and supporting tools for design and deployment of assured distributed systems that are scalable and deterministic in their execution. The project provides a top-to-bottom and end-to-end approach to such systems. Top-to-bottom as it provides a declarative high-level language for architecture modelling and property description at the top, and a fine-grained resource configuration and control at the bottom, with a tool chain in between that assures correctness of the deployment with respect to the specification. End-to-end in that the high-level architecture and properties of the distributed system are preserved in the composition of the components needed to realise the system, and that evidence that the system will exhibit the desired properties is provided by a suite of analysis and verification tools and is presented in a structured assurance case. The technology for deployment is provided by an extended separation kernel and time-triggered Ethernet networking.

INNOVATION ACHIEVEMENTS

The project delivers the following key achievements:

- The MILS-AADL declarative language for architectural modelling and specification of properties in distributed systems;
- An approach to compositional verification of properties of MILS-AADL models;
- Foundations and tool support for compositional assurance cases;
- The D-MILS platform that integrates the distributed MILS technology comprising an extended separation kernel, an extended time-triggered Ethernet, a MILS network system, and a MILS console system;
- A tool chain including a parser and translators for the annotated MILS-AADL language, an analysis and property verification suite, an assurance case constructor, and a configuration compiler for the D-MILS platform.

OVERCOMING CONSTRAINTS OF THE MARKET

Lack of awareness of the D-MILS results could limit the project results' exploitation in companies outside the consortium. Another potential impediment could be compatibility of the D-MILS tools and technologies with existing industry standards.

D-MILS aims to facilitate and promote the potential use and take-up of its results by a wide range of technology providers in addition to those in the project, and to work with standards bodies to extend existing standards and profiles to guarantee interoperability of tools and technologies that exploit the project results.

MARKET INVOLVEMENT

The D-MILS project brings the needed improvements in critical systems security and assurance by providing an environment for design, implementation, verification and certification of scalable trustworthy architectures for

Coordinator

The Open Group (UK)

Partners

Fondazione Bruno Kessler (FBK) (IT)

fortiss (DE)

Frequentis (AT)

LinuxWorks (FR)


RWTH Aachen University (DE)

TTTech (AT)

Université Joseph Fourier (FR)

University of York (UK)

D-MILS

Call  8 3 Years
(2012-11-01 to 2015-10-31)


9 Partners


5 Countries


€ 2.850.000 EU Contribution

<http://www.d-mils.org> 

distributed systems, and by providing deployment technology in the form of enhanced commercially available products.

PILOTS

The results of the project are validated on two industrial demonstrators: the Fortiss Smart Micro Grid and Frequentis Voice Services.



Towards more secure cyber-physical networks

EURO-MILS

Secure European Virtualization for Trustworthy Applications in Critical Domains

Coordinator

TECHNIKON (AT)

Partners

SYSGO (DE)

Airbus (FR)

EADS (DE)

T-Systems (DE)

EADS (FR)

Thales Communications&Security (FR)

SYSGO (FR)

University of Gent (BE)

Open university of the Netherlands (NL)

German Center for Artificial Intelligence (DE)

University Paris-Sud (FR)

OpenSynergy (DE)

Jemm Research (FR)

TU Eindhoven (NL)

The EURO-MILS project works on providing trustworthiness by design and high assurance for cyber-physical networks of embedded systems, including strong guarantees on resource isolation by means of security certification (Common Criteria-based).

The major results of EURO-MILS are the MILS architecture template, the pan-European compositional assurance approach, and a MILS protection profile and a skeleton for the MILS framework.

RECENT DEVELOPMENTS

The project has completed the MILS architectural template developed from the security-by-design point of view with a pragmatic application of the MILS principles in mind. EURO-MILS has also produced the cornerstone standard for the envisioned MILS eco-system: the MILS protection profile for separation kernel, and is currently conducting a pilot application of this standard on a European COTS product. With these two major milestones achieved, the project is building up the MILS framework to tackle the major challenge of the compositional approach for security. EURO-MILS partners have carried out survey on social and business acceptance of security and MILS approach.

VALIDATION STRATEGY

EURO-MILS executes a wide range of validation activities: a pilot application, a set of test-beds, demonstrators, publications at the international Common Criteria conference to ensure acceptance by certification practitioners.

EURO-MILS

Call  3 Years
(2012-10-01 to 2015-09-30)



15 Partners



5 Countries



€ 6.000.000 EU Contribution



<http://www.euromils.eu>

HAVE A LOOK AT

FIRE organizes a final conference in Brussels in October 2014.

<http://www.trustworthyictonfire.com/activities-and-events-schedule/fire-s-final-conference>

An economically sustainable European identity management infrastructure



FutureID

Shaping the future of electronic identity

«We are trying to build free and open market place for federated identity management or identity management in general, so we develop the building blocks that could be used to provide interoperability between different standards. [...] Our goal in the end is that the user can use any token of his choice to log into basically any service on the Internet. This is of course not an easy task, it requires lot of "plumbing" to put things together and to translate from one protocol to another». **Heiko Rossnagel, project coordinator**

The FutureID project designs a flexible and privacy-aware identity management infrastructure for Europe. The main goal is to develop building blocks that could be used to provide interoperability between different identity management standards, and to organize an open marketplace for identity management where many service providers and identity providers can operate.

RECENT DEVELOPMENTS

The development of most components in support of qualified signature and authentication have been completed in a first minimal version or are at an advanced stage. First abbreviated system tests have been performed. This also includes an innovative trust infrastructure that is based on the Domain Name System. Also special emphasis has been put on mobile scenarios. Ample work has gone in the management of requirements in a semantic wiki and the setup of a comprehensive test and continuous integration infrastructure. A first feedback loop has evaluated the architecture against the requirements.

VALIDATION STRATEGY

The project considers testing the cornerstone of its validation. Each tool undergoes heavy testing, with a specific testing task in each work package, and two dedicated testing work packages for the client and the server side test-beds.

FutureID has developed a distributed test-bed running automatically; the tests can be run from virtually everywhere. Another dedicated work package monitors the requirements fulfilment, and there will be two pilot applications implemented.

Coordinator

Fraunhofer-Gesellschaft (DE)

Partners

SK (EE), Technical University of Denmark (DK), University of Stuttgart (DE), IBM Research (CH), Catholic University of Leuven (BE), Technical University of Darmstadt (DE), AGETO (DE), EEMA (BE), Graz University of Technology (AT), ULD (DE), Norsk Regnesentral (NO), ATOS (ES), University of Newcastle upon Tyne (UK), Giesecke & Devrient (DE), Infineon Technologies (DE), Comarch (PL), ECSEC (DE), Radboud University Nijmegen (NL)

FutureID

Call  3 Years
(2012-11-01 to 2015-10-31)


19 Partners


11 Countries


€ 9.992.825 EU Contribution

<http://www.FutureID.eu> 

HAVE A LOOK AT

FutureID is co-organizing the Open Identity Summit 2015 (<https://www.openidentity.eu>) in November that is collocated with ISSE 2015 in Berlin. FutureID will among others also be present at Trust in the Digital World (<http://trustindigitallife.eema.org/>), the Cybersecurity and Privacy Innovation Forum (<https://www.cspforum.eu/2015>) and the European Association of Biometric's Research Project Conference (<http://www.eab.org/events/program/79>)



GEMOM

Genetic message oriented secure middleware

Coordinator

CNIT (IT)

Partners

VTT Technical Research Centre (FI)

Norsk Regnesentral (NO)

Queen Mary University of London (UK)

TXT e-Solutions (IT)

Diginus (UK)


Datel Consulting (IE)

Hewlett-Packard (IT)

Q-Sphere (UK)

JRC Capital Management Consultancy & Research (DE)

GEMOM

Call  2,5 Years
(2008-01-01 to 2010-06-30)


10 Partners


6 Countries


€ 3.300.000 EU Contribution

 <http://www.gemom.eu>

SUMMARY

The focus of GEMOM is the significant and measurable increase in end-to-end intelligence, security and resilience of complex, distributed information systems. Existing technologies are crude, not scalable and not suited for what will be required in the future. There is neither adequate robustness nor resilience appropriate for future real-time systems in particular, and the project will provide solutions to overcome these limitations to secure messaging. Fault tolerance will be looked at in a more dynamic way.

GEMOM's definition of intelligence and resilience draws attention to the fact that there can be insensitivity or low awareness of faults. These faults could result in the deterioration of the functional profile of the informational system, of the volumetric profile, or of the security profile. It also brings into question the availability of support for a reconfiguration back to an efficiently working system.

The primary objective of GEMOM is to be able to rectify such vulnerability to faults. This will be through **researching, developing and deployment of a prototype of a messaging platform that is evolutionary, self-organising, self healing, scalable and secure**. GEMOM will be resilient and be able to utilise redundant modules (hot-swap or switchover) instantly without information loss. These resilience features will allow specialist, independent system actors, (viz. watch-dogs, security and situation monitors, routers, and other optimisers,) to remove or replace compromised nodes from the broader network instantly and without compromising higher level functionality and security. GEMOM considers the Publish-Subscribe variant of Message Oriented Middleware to be the predominant one and will focus on issues surrounding that kind of messaging. For completeness GEMOM would provide a synchronous Request and Reply overlay as well.

By concentrating on the notion of a "fault" GEMOM expects to make advances in the security of messaging. In addition to the intuitive understanding of what a fault might be - whereby any actor stops being operable, connection is lost etc, GEMOM extends the notion of fault to include compromised security or inadequate bandwidth availability in the first iteration. The final iteration will also include the compromised abstract notion of "resource".

GOALS & STRATEGIES

The core scientific focus of GEMOM is the significant and measurable increase in end-to-end intelligence, security and resilience of complex, distributed information systems.

GEMOM's definition of intelligence and resilience include:

- Insensitivity or significant reduction in sensitivity to individual and sometimes multiple faults in the system. A fault is defined as any deterioration of the functional profile of the information system, the volumetric profile, and the security profile;
- Support for a reconfiguration as an efficient system.

The advances that GEMOM proposes to make to the area of messaging revolve around the notion of a "fault". In addition to the intuitive understanding of what a fault might be, whereby any actor stops being operable, connection

is lost etc, GEMOM extends the notion of fault to include compromised security or inadequate bandwidth availability in the first iteration and compromised abstract notion of “resource” in its final iteration.

Core research focus of GEMOM is ultra-resilience of messaging. GEMOM analyses the following core issues that underpin ultra resilience and so could compromise it as well:

- **Reliability of message sourcing and delivery.** To accommodate this GEMOM offers to handle redundant message feeds, where needed, and redundant delivery paths. In the event of failure switch over to redundant resource would be effectively instantaneous and with no information loss. In addition to entire message broker redundancy GEMOM offers redundancy of certain subsets or messaging segments. As part of its self-healing when redundant components are switched to and used, GEMOM finds and primes other nodes, feeds or paths as new redundant components. In short, GEMOM ensures that there are no single points of failure even as new nodes become compromised and so rendered alien and isolated.
- **Scalability with respect to message volumes.** GEMOM will ensure that scalability is not compromised as redundancy is utilised. Switchover to redundant components will preserve scalability.
- **Replicating structural and dynamic properties of security metrics.** One particular GEMOM setup might be configured with a certain security layout in place. GEMOM will research issues and deploy innovative solutions to ensure that the security profiles of overall system and individual message paths and dynamics are not compromised as a result of failovers. Namely, GEMOM will be capable of fully replicating structural and dynamic properties of security policies.
- **Process zoning and overall encapsulation to an arbitrary level.** Where the economy of the implemented solution carries higher weighting GEMOM allows for separation of cheaper messaging (still scalable, resilient and self-healing) on one side but fully fledged monitoring, management and maintenance on another side. Namely, GEMOM allows for process zoning and overall encapsulation to an arbitrary level.
- **Pre-emptive vulnerability testing and vulnerability updating.** Whether by accident or as the result of deliberate cyber attack, components executing on different computers across different trust boundaries may interact in an unforeseen way or expose a vulnerability that an attacker could exploit. Pre-emptive detection of known and unknown vulnerabilities needs tools that can analyse the deployed middleware, client server applications and web service based applications both statically and dynamically, and this will be provided by GEMOM. This will also allow checking for new vulnerabilities when they are reported.

Message oriented middleware acts at a trust boundary and is often not just a passive entity. It combines and transforms data and sends it to other components. Message oriented middleware is therefore an important location to be guarded and for guarding the components with which it interacts. GEMOM will investigate and develop novel techniques that can automate the intelligent checking of the deployed GEMOM system for robustness to misconfiguration, erroneous data and vulnerabilities to cyber attacks in the context of the deployed environment.



MASTER

Managing assurance, security and trust for services

Coordinator

ATOS (ES)

Partners

SINTEF (NO)

IBM Research Lab (CH)

University of Stuttgart (DE)

ETH (CH)

University of Trento (IT)

Dublin City University (IE)

British Telecom (UK)

ANECT (CZ)

ENGINEERING (IT)

San Raffaele Foundation (IT)

Deloitte (FR)

CESCE (ES)

MASTER

Call  3 Years
(2008-02-01 to 2011-01-31)


13 Partners


9 Countries


€ 9.300.000 EU Contribution

OBJECTIVES

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

INNOVATION TARGETS

MASTER has delivered the following key results:

- **The MASTER methodology** that describes how an organization can derive specific activities to be done and control objectives from high level regulations and policies;
- **The MASTER design workbench** – a tool to translate high-level regulations and policies into low-level policies that control management process in an organization.

IMPACT

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



MATTHEW

Multi-entity-security using active Transmission Technology for improved Handling of Exportable security credentials Without privacy restrictions

Today users not only have multiple mobile devices, but they also use these devices to carry their credentials (e.g., the transport tickets and passes). The devices also have relatively short lifecycles – some users tend to change their smartphones regularly. In this setting the problem of transporting credentials across the devices while keeping their confidentiality and integrity and respecting the user privacy is especially important.

The MATTHEW project is set to design privacy-preserving security applications utilizing the novel combinations of active Near Field Communication (NFC) and hardware protection provided by secure elements in mobile devices and ensuring transferability of these applications and their credentials across devices.

INNOVATION ACHIEVEMENTS

MATTHEW delivers:

- An enhanced active transmission technology for NFC communications across mobile devices;
- A proof-of-concept framework for credentials transferring across mobile platforms;
- Close-to-exploitation prototypes of novel payment methods that are easily transferrable from one device to another and a multi-key access control system.

CONSTRAINTS TO SUCCESSFUL EXPLOITATION

MATTHEW envisages the usage of hardware protections to store the credentials, yet currently the secure element ecosystem for mobile devices is closed. Each secure element in the device has its owner that is today not disposed to give other stakeholders the access rights to the storage. Most likely the struggle between security providers on the platform will not be solved during the run-time of MATTHEW, thus various flavours of how to deal with security credentials are taken into account in MATTHEW.

MITIGATION STRATEGIES

The project considers that once there is an opportunity for secure credentials exchange, the ecosystem will react favorably to it. Moreover, many of the project results will be very close to exploitation by its delivery, because the industrial partners responsible for these results have already clear business cases in mind.

IMPACT

The results of MATTHEW will be appealing to the end users because they will be able to easily switch the mobile devices while retaining all their credentials. **The results of MATTHEW will also give rise to the new wave of NFC applications by providing more reliable and privacy-preserving communication means.**

The main exploitation target can be identified in two layers: the security hardware vendors, represented in the project by Infineon Technologies, and companies like Gemalto, providers of operating systems and secure applications. **The results of MATTHEW will be appealing to end users like banks and their customers because they will be able to easily switch the mobile devices while retaining all their credentials.**

Coordinator

Infineon Technologies Austria AG (AT)

Partners

Technical University of Graz (AT)

Cryptoexperts (FR)

Infineon Technologies AG (DE)

AMS (AT)

Technikon (AT)

Institute of Microelectronic Applications (CZ)

Gemalto (FR)

MATTHEW

Call  3 Years
(01.11.2013 to 31.10.2016)


8 Partners


4 Countries


€ 3.600.000 EU Contribution

<http://matthew-project.eu/> 

USE CASES

MATTHEW has three case studies: **the mobile banking scenario led by Gemalto; the multi-key access control driven by IMA, and the transferrable credentials driven by CryptoExperts.**



MICIE

Tool for systemic risk analysis and secure mediation
of data exchanged across linked CI information infrastructures

Coordinator

Selex (IT)

Partners

University of Coimbra (PT)
University of Bradford (UK)
Henri Tudor Research Center (LU)
CRAT University of Rome (IT)
University of Rome Tre (IT)
ENEA (IT)
PIAP (PL)
Israel Electric Corp (IL)
Itrust consulting (LU)
Multitel ASBL (BE)

MICIE	
Call 	2,5 Years (2008-09-01 to 2011-02-28)
	11 Partners
	7 Countries
	€ 2.448.164 EU Contribution
	http://www.micie.eu

OBJECTIVES

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

INNOVATION TARGETS

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

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

IMPACT

The MICIE project results are directly in line with the EU initiative to establish a Critical Infrastructure Warning Information Network (CIWIN), contributing to safety of the EU society.

The energy distribution domain was chosen as an application for validation of the project results. The project has evaluated whether the MICIE tool could increase the quality of service in this domain. After analyzing the communication fault events and their influence on the quality of service of the electric energy supply in presence of the MICIE tool and without it, the consortium has concluded that the MICIE technology can increase the quality of service by assisting the operator in identifying faults and countermeasures.

A risk-based approach learning from new threats



PANOPTESSEC

Dynamic Risk Approaches for Automated Cyber Defence

Many organizations today fail to secure their systems and networks against cyber attacks because of the complexity of the infrastructure and the lack of the qualified security personnel. **PaNoPteSec is aiming to design a cyber defense decision support system** that will support organizations in detecting the attacks and responding to them. The main idea behind the new system is that it will be risk-based and will learn dynamically in order to respond to the new threats and new attacker capabilities.

INNOVATION ACHIEVEMENTS

PANOPTESSEC delivers a prototype suite of integrated technologies for:

- a cyber security data collection and correlation;
- a risk quantification and assessment;
- mitigation response prioritization and activation;
- visualization support for security operators.

OVERCOMING CONSTRAINTS OF THE MARKET

Although security awareness has increased in Europe in recent years, the issues of fiscal restraint in a slow market economy continue to limit security spending. Therefore organizations might not be willing to invest into a full fledged PANOPTESSEC suite and the security sensors needed.

The project aims to deliver a near-market-ready system that will be suitable for exploitation for project partners and other interested organizations. The final PANOPTESSEC demonstrator will support further exploitation of the solution by critical infrastructure customers as well as transportation, banking/finance, government and defense markets.

IMPACT

The results of the project are in line with the EU NIS Strategy and the National Strategies of the Member States; and the technologies delivered by the project are in demand by the organizations.

PLLOT

The project validation is planned through demonstrations in both simulated and operational environments for critical infrastructure protection. **A simulation environment will be built to mimic cyber-security sensor capabilities of three operational environments (enterprise ICT, electric power distribution, and clean water distribution).** A final demonstration will involve live data feeds from these operational environments to assess system response compared to existing operational tools and processes.

Coordinator

Institute Mines - Telecom (FR)

Partners

ACEA (IT)

Epistemica (IT)

University of Rome La Sapienza (IT)

Ecole Supérieure D'Electricité (FR)

RHEA System (BE)

Alcatel-Lucent Bell Labs (FR)

University of Lübeck (DE)

PANOPTESSEC

Call  3 Years
(01.11.2013 to 31.10.2016)


8 Partners


4 Countries


€ 5.249.986 EU Contribution

<http://www.panoptesec.eu/> 



Secure Provisioning of Cloud Services
based on SLA Management

SPECS

Secure Provisioning of Cloud Services based on SLA management

Coordinator

CerICT (IT)

Partners

Technical University of Darmstadt (DE)

Institute E-Austria Timisoara (RO)

Cloud Security Alliance (UK)

XLAB (SL)

EMC Information Systems International (IE)

SPECS

Call  3 Years
(2013.11.01 to 2016.04.30)



6 Partners



6 Countries



€ 2.400.000 EU Contribution



<http://specs-project.eu/>

The Cloud offers attractive options to migrate corporate applications without the corporate security manager needing to manage or secure any physical resources. While this “ease” is appealing, several security issues arise:

- With security sensitive data residing remotely with the Cloud Service Provider (CSP), can access of unauthorized CSP personnel to your data be restricted?
- How does one assess a CSP's ability to meet the corporate security requirements and the security trades-offs offered by different CSPs?
- Can one monitor and enforce the agreed Cloud security levels with the CSP?

No comprehensive and easily usable solutions exist for these issues.

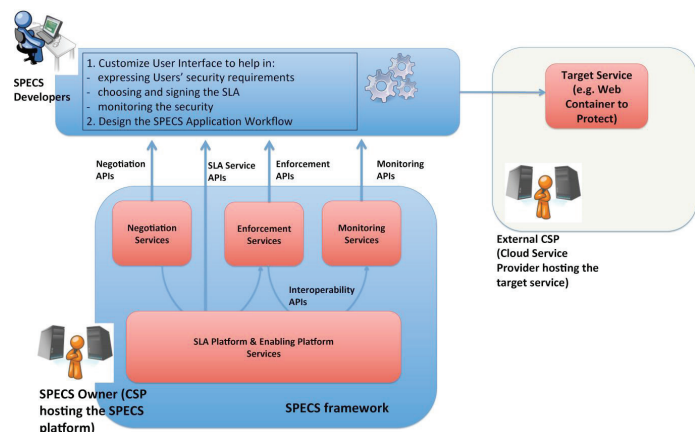
SPECS solves this problem, offering:

- Mechanisms to specify Cloud security requirements and assess the standalone and comparative security features offered by CSPs.
- Ability to integrate desired corporate security services (eg. credential and access management) into Cloud services.
- Systematic approaches to negotiate monitor and enforce the security parameters specified in Service Level Agreements (SLA).
- Approaches to develop and deploy security services that are “Cloud SLA-aware”, implemented as an open-source Platform-as-a-Service (PaaS).

Providing such comprehensible and enforceable security assurance by CSP's is a critical factor to deploy trustworthy Cloud ecosystems. Targeting ICT-2013.1.5 “Trustworthy ICT”, **SPECS will develop and implement an open source framework to offer Security-as-a-Service, by relying on the notion of security parameters specified in Service Level Agreements (SLA) and providing the techniques to systematically manage their life-cycle.**

The SPECS framework addresses both CSP's and users to provide techniques and tools for:

- Enabling user-centric negotiation of security parameters in Cloud SLA, along with a trade-off evaluation process among users and CSPs, in order to compose Cloud services fulfilling a minimum required security level.



- b) Monitoring in real-time the fulfillment of SLAs agreed with CSPs, notifying both users and CSPs, when a SLAs not being fulfilled.
- c) Enforcing agreed SLA in order to keep a sustained Quality of Security (QoSec) that fulfills the specified security parameters. SPECS' enforcement framework will also "react and adapt" in real-time to fluctuations in the QoSec by advising/applying the requisite countermeasures.

The proposed framework has an open-source core, and offer simple interfaces to motivate its adoption. It will offer a set of reusable PaaS components for service developers to enable them to integrate SPECS' SLA-oriented security mechanisms into existing Cloud services.

Using real case studies SPECS will demonstrate that the SPECS framework and architecture can be integrated "as-a-Service" into real life Cloud environments, with a particular emphasis on small/medium CSPs and end users.

INNOVATION ACHIEVEMENTS

The SPECS project will provide:

- The SPECS platform: a running platform to execute and manage SPECS Services and Applications, Offers SPECS Core services (Negotiation, Monitoring, Enforcement).
- The SPECS framework: an open source framework to develop SPECS Applications by using the SPECS Core services, Offers Commercial-off-the-shelf Security mechanisms and controls, Provides Security SLA representation.
- Example Application: four applications developed using the SPECS framework and running over the SPECS platform, they address specific end-user communities Security Requirements.

OVERCOMING CONSTRAINTS OF THE MARKET

One of the potential constraints to successful exploitation of the project results is the high dynamicity of the cloud market and the constant changes in technology. Another constraint is the current lack of SLA standards that offer the right level of service description details.

SPECS actively engages with the standardization bodies and participates in the process of building the SLA standards.

IMPACT

The platform and SLA negotiation, management and enforcement approaches provided by SPECS will allow organizations in Europe to have more trust in the cloud services security and will ensure growth of this market sector.

USE CASES

The project will be validated on **four use cases**.

All partners collaborate on a SPECS Application able to offer Secure Web Containers.

XLAB is the leader of a task devoted to build a SPECS Application able to offer Data-as-a-Service Security SLAs, with features like client side encryption. EMC2 is a leader of the task devoted to build a SPECS Application that offer Security SLAs for the next-generation data centers.

The XLAB and EMC2 will collaborate on building a SPECS Application able to offer identity management solutions, covered by Security SLAs.

HAVE A LOOK AT

The SPECS Project web page www.specs-project.eu hosts the link to all the relevant standards and information related to Cloud Security and Security SLAs.

Follow SPECS activities on Twitter (<https://twitter.com/FP7SPECS>) and LinkedIn (<https://www.linkedin.com/groups/FP7-SPECS-project-Secure-Cloud-7475930>)



A static code analysis protecting industries

STANCE

A Source code analysis Toolbox for software security AssuraNCE

Coordinator

CEA-LIST (FR)

Partners

Graz University of Technology (AT)

Trusted Labs (FR)

Dassault Aviation (FR)

Catholic university of Leuven (BE)

Search-Lab (HU)

ARTTIC (FR)

Infi neon Technologies (DE)

FOKuS at Fraunhofer (DE)

Thales Communications&Security (FR)

STANCE

Call  8 3 Years
(2012-10-01 to 2016-03-30)


10 Partners


5 Countries


€ 3.800.000 EU Contribution

 <http://www.stance-project.eu>

«In Europe we have industries and institutions capable of improving security of our software. It not only critical software can be improved; but also the software that are used every day. We have the capabilities to improve their security, but we need to federate these capabilities for helping our industry and indirectly demonstrating and increasing the confidence of European citizens in software and in device driven by software.

There is also a security market and there is much room left for companies to innovate and implement new products to increase security of software in so many applications».

Armand Puccetti, project coordinator

Nowadays critical software security vulnerabilities - such as Heartbleed - are discovered regularly.

These bugs often lead to significant monetary and reputation losses for the companies and the end-users affected. Yet these bugs could be avoided if static code analysis techniques were used regularly. In practice these techniques are used on a daily basis by industries developing critical software, but are not widely used in other fields. **The STANCE project aims to develop a set of techniques and tools for static code analysis that will be ready for use at industrial level.**

INNOVATION ACHIEVEMENTS

STANCE delivers a methodology and a toolkit to cover most of the features of C, C++ and Java programming languages that will allow the analysis of security properties on source code of complex software systems.

MARKET INVOLVEMENT

The STANCE code analysis toolbox and supporting formal methods will increase the trustworthiness and the cost-effectiveness of existing industrial processes for security validation. These innovations will improve the domain of software security assurance, and impact the trustworthiness of software systems.

OVERCOMING CONSTRAINTS OF THE MARKET

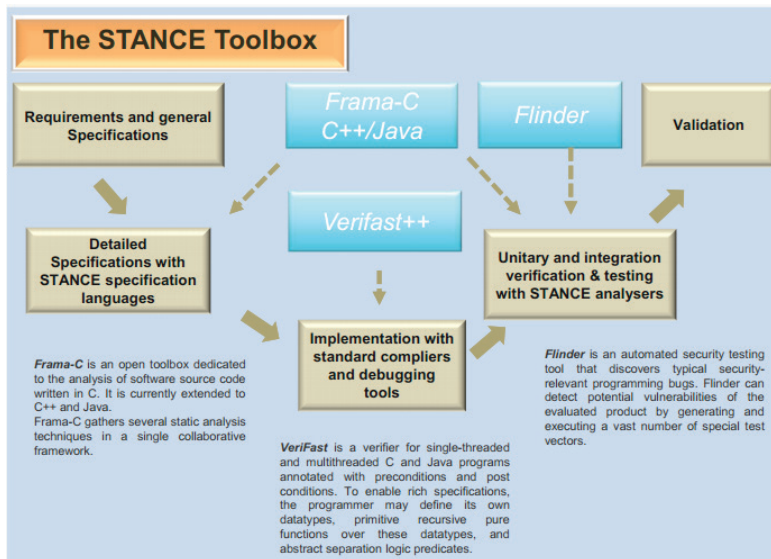
The project considers that there are two main gaps to the adoption of its result. The first gap is the level of maturity of the tools produced. The second gap is related to the industry perception of static analysis tools – these tools are not considered as very important for most organizations.

STANCE aims to push the maturity of the technologies developed by the project, as well as by follow-up projects, e.g., under the umbrella of EIT ICT Labs or H2020 for instance. Regarding the industry perception, the project works hard on disseminating its outcomes and products, while also expecting that policy based incentives for usage of these tools in industry might considerably increase the demand for the STANCE results and similar tools.

PILOTS

The project plans to validate its results via use cases spanning from the avionics domain (aircraft maintenance by Dassault Aviation) to a networking ap-

plication based on OpenSSL (this is the case of Thales communications) and to the development of TPM-based components for embedded platforms (by TU Graz and Infineon AG).





TAMPRES






TAMper Resistant Sensor node

Coordinator

IHP Innovations for High Performance
Microelectronics (DE)

Partners

NXP Semiconductors (BE)
NXP Semiconductors (DE)
Catholic University of Louvain (BE)
France Telecom (FR)
ETH (CH)
Graz University of Technology (A)
Coalesenses (DE)

TAMPRES	
Call  3 Years (2010-10-01 to 2013-09-30)	
 8 Partners	
 5 Countries	
 € 2.959.465 EU Contribution	
 http://www.tampres.eu/	

HAVE A LOOK AT

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

OBJECTIVES

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

INNOVATION ACHIEVEMENTS

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

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

MARKET ACCEPTANCE GAPS

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

MITIGATION STRATEGIES

The project engages into various activities to promote its results and open up the market. In July 2013 TAMPRES has conducted a workshop with potential customers to present the project solutions. The NXP partner in the TAMPRES consortium will adopt some of the developed solutions in their chips.

IMPACT

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

ZOOM IN

The developed secure components are tested using AFPD designs. The integrated prototype of a secure microcontroller is implemented on an ASIC chip. Notice that TAMPRES comprises the leading industry partners in chip hardware security. **The partners have already acquired four patents for their technology.**

UAN

Underwater acoustic network

OBJECTIVES

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

INNOVATION TARGETS

UAN has produced the next key innovative results:

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

IMPACT

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

Coordinator

CINTAL (PT)

Partners



SELEX (IT)

SINTEF (NO)

FOI Sweden Defense Research Agency (SE)

ISME at University of Genova (IT)

KongsBerg Maritime (NO)

UAN	
Call  7	4 Years (2008-10-01 to 2011-09-30)
	
6 Partners	
	
4 Countries	
	
€ 2.950.000 EU Contribution	

HAVE A LOOK AT

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

VIKING

Vital infrastructure, networks, information and control systems management

Coordinator

TABB (DE)

Partners

E.ON (DE)

ETH (CH)


MML Analysis and Strategy (SE)

The University System of Maryland Foundation (US)

KTH (SE)

Astron Informatikai (HU)

VIKING

Call  3 Years
(2008-11-01 to 2011-11-30)



7 Partners



5 Countries



€ 1.824.950 EU Contribution



<http://www.vikingproject.eu>

OBJECTIVES

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

INNOVATION TARGETS

VIKING has developed the next key innovations:

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

IMPACT

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

HAVE A LOOK AT

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

The results of the project are summarized in the VIKING final report available on the VIKING web page. Furthermore, the project has made a movie illustrating one of the VIKING Story Boards:

http://www.youtube.com/watch?v=Y_ifu65FdXo

(also available at the project website)

4

COMMUNITY BUILDING ACTIVITIES PROJECTS



Community Building Activities Projects

Network of Excellence

Network of Excellence projects belong to this area, as they contribute to strengthen scientific and technological excellence on ICT Security and Privacy, by creating new knowledge through research activities, maintaining a long lasting research community and supporting conferences, infrastructures and cooperation among partners, as well as all the facilities required for the development of a research community.

NESSOS project (Call 5) coordinates and fosters research activities for secure Future Internet software services and systems engineering and promotes education activities in this domain. The NESSoS researchers performed community-wide activities, realigned their research interests and worked together in several successful initiatives. A joint virtual research lab (JVRL) has been set up for collaborative working. NESSoS is now a world-wide community with the creation of the new IFIP WG 11.14 on Secure Engineering that represents a cornerstone in the long standing research community and the development of a consolidated research roadmap in collaboration with the NESSoS Industry Advisory Board members. NESSoS researchers actively contributed also to the Network and Information Security Platform (NIS). The NESSoS common body of knowledge is up and running: it has been populated with several knowledge objects, its usability analysis has been performed and the process of opening it to the wider audience is on-going.

Identifying threats and vulnerabilities of the Future Internet is the aim of SYSSEC project (Call 5), who delivered the Red Book¹ - a Roadmap for Systems Security Research - allowing to identify the main threats, topics and concerns in the Fu-

ture Internet. A dynamic mobile malware detection has been developed by the Vienna University of Technology partner: Andrubis² is a dynamic analysis environment for Android applications that provides a publicly available submission interface for security researchers and average mobile users alike. Internally, it makes use of the TraceDroid framework, developed by Vrije University of Amsterdam. SysSec has created a common curriculum to be used by University Professors. Spearhead of this is the "10K Students Challenge"³, which aims to teach 10,000 students about buffer overflows and cyber security, SysSec's common curriculum expects to have a real impact in the next generation of software developers.

ECRYPT II is a Network of Excellence project funded by Call 1 in Cryptography. It ensures integration of the EU research in this area into academia and industry, developing common tools and benchmarks, and fostering the EU cryptography community. The ECRYPT II research roadmap is motivated by the changing environment and threat models in which cryptology is deployed, by the gradual erosion of the computational difficulty of the mathematical problems on which cryptology is based, and by the requirements of new applications and cryptographic implementations. In order to reach this goal, 11 leading players proposed to integrate their research capabilities within three virtual labs focusing on symmetric key algorithms, public key algorithms and protocols, and hardware and software implementation. They will be joined by more than 20 adjoint members to the network who will closely collaborate with the core partners. ■

¹ <http://www.red-book.eu/>

² <http://analysis.iseclab.org>

³ <http://10kstudents.eu/>

Trust in Digital Life

On 24 November 2008, Philips, Microsoft, Nokia and Gemalto took the initiative to establish the Trust in Digital Life Partnership⁴. The coordination action **ACTOR**, funded within the Call 5, supports the TDL Partnership raising awareness of research and its results of trustworthy ICT and establishing a network by involving additional members for the definition of a SRA and implementation through research projects.

ACTOR's follow-up, **ATTPS** (Call 8), will offer a validation environment that service providers can use to evaluate acceptability of their products by end-users. It aims at achieving the trust paradigm shift by making people and decision makers more

aware about the secure and trustworthy solutions. The project supports pragmatic actions such as developing and testing of generic trust architectures and integration pilots. Moreover, ATTPS promotes the existing technologies in this area, contributes to interoperability and standardization in the EU, and fosters the willingness of the stakeholders to pay for these technologies. This project is also developing a generic trust architecture for trustworthy services and providing a real test-bed environment that can be used externally to quickly validate third-party solutions, which can help them to understand better the business needs and engage with potential customers. ■

Enhancing the Standardization Process

Many EU and international efforts are being aimed towards improving security, assurance, transparency and simplifying legal compliance. The action plan proposed in 2012 in the European Cloud Strategy by the EC and implemented in 2013-14, is producing positive contributions in key areas like security, definition of fair terms and conditions, liability, Service Level Agreements (SLA), and Privacy compliance. Notable are also the results in the international cooperation and community efforts such as the European Cloud Partnership, Helix Nebula, the cooperation with Brazil/USA/Japan, the participation of EU-driven effort to the standardization community and the cooperation between the research consortia funded under the FP7 programme.

The **CIRRUS** project (Call 8) aims at supporting the definition of such an action plan for increasing the level of trust in Cloud computing. Its contributions focus on the Cloud security standardization and certification efforts, with the goals of supporting on-going research projects and coor-

dinate a dialogue that will lead to a convergence of such efforts. Among the main outcomes that CIRRUS is planning to achieve there is 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 ANIKETOS, Assert-4SOA, CUMULUS and PCAS.

STREWS (Call 8) will dedicate itself to a roadmap for future research and standardization for Web security. STREWS created a comprehensive Web Security Guide that gives an overview of the current Web and the expected developments in the near future. From this basis, STREWS developed a Web security vulnerability landscape by describing the Web assets, attacker capabilities and commonly used attacker models. Moreover, the STREWS project links European security and trust related research and development with ongoing standards and development work for the Web in IETF and W3C. ■

Creating International Connections among EU projects and other International Programmes

There are not so many projects addressing coordination with related national or regional programmes. In this area some projects can be named: BIC, CYSPA and partially FIRE. Yet these projects have addressed alignment with non-European research programmes.

Coordination of EU research in trustworthy ICT and alignment of the EU vision with research programmes in Brazil, India and South Africa are the

objectives of **BIC**. BIC responded to Call 5 with the priority towards the international co-operation in the fields of cyber security. Successful models developed by the project partners will be used to engender cooperation of EU researchers and program management in Trustworthy ICT with their peers in countries who have already signed Science and Technology (ST) agreements, namely Brazil, India and South Africa.

⁴ <http://www.trustindigitallife.eu/>

CYSPA is a project from Call 8 that aims to set up an European Cyber Security Protection Alliance, which aim is to bring together EU stakeholders to articulate, embody and deliver the concrete actions needed to reduce cyber disruption. CYSPA is using this opportunity as seed funding to launch an Alliance with a goal of self-sustainability beyond the end of the project itself. Moreover, this project aims to review the existing national activities in cyber security and to analyze the impact of cyber threats across four important sectors: E-Government, energy, finance and transport, providing sector-specific guidelines for protection. The project also collaborates with other relevant communities, including the NIS Platform, and tries to connect with a large variety of stakeholders outside the project itself.

EFFECTS+ (Call 5) and **SECCORD** (Call 8) aimed at conducting a detailed analysis of the work of the FP7 ICT projects mentioned in this document, providing evidence of their valuable and meaningful results and potential impact. The final purpose is to demonstrate the dividends, outputs and benefits resulting from the investment in T&S research. Moreover, these projects planned different actions in order to provide greater visibility of T&S research programme, also through a high-profile annual conference (CSP EU Forum); the goal is that these become a recognizable brand. Visibility and outreach will be extended by building on an already established community of interests to include relationships with industry and T&S initiatives of member states. ■

Dealing with the Security Market

Call 8 project **FIRE** aims at improving the European industrial competitiveness in the trustworthy ICT markets by analyzing the gap between industry and research and trying to reduce it through a variety of mechanisms. It aims at capturing the user needs to develop a research agenda that will inform the Horizon 2020 research Programme; identifying the best practices and stimulating commercially compelling cooperation between successful regional clusters; developing both formal and informal mechanisms to support research and innovation activities by connecting researchers and users on a transnational basis. FIRE delivers a report on the industry sector research needs and an infrastructure including all segments of the ICT security value chains. This infrastructure includes the Pan-cluster research Network and the industrial and commercial Networks (ICNs) that voice the industry needs. ICNs are dedicated to the key industry sectors: energy, finance, healthcare, mobile communications, and e-Government. R&D projects in Europe deliver excellent technology, yet often this technology fails to reach the market, or there is insufficient market demand. The **IPACSO** project (Call 10) investigates some of the reasons behind the market readiness and demand of cyber security and privacy technologies developed in research organizations, and builds an innovation framework that will support inno-

vation to market transfer. The project will develop an innovation framework for cyber security and privacy technologies that will comprise guiding principles for innovators in the domain, to support them in identifying and exploring market opportunities and a market knowledge-base of privacy and cyber security products/services. IPACSO has also established an award for cyber security and privacy innovators recognising excellence in innovative research, solutions and approaches to secure our privacy and protect our assets and critical infrastructures.

An analysis of the security market will also be conducted by **CAPITAL**. This Call 10 project will provide a market study of cyber security and privacy technologies in the eight emerging areas (cloud computing, security and privacy incident management, cyber security and privacy engineering, Internet of Things, mobile computing, Big Data, critical industrial systems, online trust and transparency for privacy) that is based on a stakeholder survey conducted by CAPITAL to gather information about cyber security and privacy risks faced by EU organizations. Furthermore, CAPITAL brings together the leading European organizations in cyber security in order to deliver a strategic research agenda that will allow to understand the priorities and to tackle the most important problems for European security and privacy. ■

Policy and Research Challenges on Security

Call 1 **THINK-TRUST** project's main aim is to bring together the European R&D community in the field of Trust, Security and Dependability (TSD) and other identified important correlative non-technical stakeholders that have a vested interest and can contribute in a meaningful way in the

development of present and future programmes of Research and Development for ICT for Trust, Security and Dependability. The project engaged with a wide range of stakeholders (technical and non-technical) with the objective of providing visionary guidance on policy and research chal-

allenges in the field of Security and Trust in the Information Society. These stakeholders were primarily engaged through the RISEPTIS Advisory Board (Advisory Board for Research and Innovation in Security, Privacy and Trustworthiness in the Information Society) which comprised leading experts in the field.

GINI-SA (Call 5) is driven by the vision of a Personalised Identity Management ecosystem where people will control their own Individual Digital Identity (INDI) space. Individual persons will have the ability to establish and manage personalised digital identities, which they will own, linking them to verifiable and authoritative national data registries. They will be able to present their chosen, verified digital identity to other physical persons or legal entities with which they wish to establish trust relationships in order to perform transactions for personal, business or official purposes. GINI-SA has examined the technological, legal, regulatory and privacy-related dimensions of the gap between the current state of the art and the vision for an INDI ecosystem beyond 2020. GINI-SA partners further identified gaps between the existing conditions and the envisaged ecosystem in each of those different – but entangled – streams. The actions defined by the GINI-SA Roadmap have been identified as required for overcoming those gaps. The initiatives

are organised in terms of actions to be taken by the different main stakeholder categories, including the research community, public actors and industry/the market.

The mission of the **PRIPARE** project (Call 10) is twofold: to facilitate the application of a privacy and security-by-design methodology that will contribute to the advent of unhindered usage of the Internet against disruptions, censorship and surveillance; and to foster a risk management culture through educational material targeted at a diverse group of stakeholders. To this end the project will define the PRIPARE Methodology: a privacy and security-by-design software and systems engineering methodology, developed using the combined expertise of the industry and the research community, applicable by companies and organizations of all sizes during the full lifecycle of the system and for any personal data which may be collected, stored or processed, including special categories of personal data (sensitive data). This methodology is heavily influenced by existing standards (e.g. ISO29100, 29101 or OASIS PMRM and PbD-SE). One of the PRIPARE consortium members also contributes to the development of an ISO standard on privacy impact assessment (ISO/IEC WD 29134). The project will also support FP7 and Horizon 2020 research projects at their privacy decisions. ■

Community Building Activities

Projects Summary

Project	Coordinator	EU Contribution	Call	Website
NESSOS	CNR (IT)	€ 3.8M	5	http://www.nessos-project.eu
SYSSEC	FORTH-ICS (GR)	€ 2.5M	5	http://www.syssec-project.eu
ATTPS	BICORE (NL)	€ 1.9M	8	http://www.attps.eu
CIRRUS	ATOS (ES)	€ 680K	8	http://www.cirrus-project.eu
CYSPA	European Organisation for Security (BE)	€ 1.7M	8	http://cyspa.eu
FIRE	AMETIC Spain (ES)	€ 1.3M	8	http://www.trustworthyictonfire.com
STREWS	W3C/ERCIM (FR)	€ 790K	8	http://www.strews.eu
GINI	IKED (SE)	€ 725K	5	http://www.gini-sa.eu
ACTOR	BICORE (NL)	€ 800K	5	http://www.trustindigitallife.eu/actor.html
ECRYPT II	Catholic University of Leuven (BE)	€ 3M	1	http://www.ecrypt.eu.org
BIC	Waterford Institute of Technology (IR)	€ 750K	5	http://www.bic-trust.eu
THINK TRUST	Waterford Institute of Technology (IE)	€ 580K	1	http://www.think-trust.eu
IPACSO	Waterford Institute of Technology (IE)	€ 950K	10	http://ipacso.eu/
CAPITAL	EOS (BE)	€ 1M	10	http://www.capital-agenda.eu/
PRIPARE	Trialog (FR)	€ 1M	10	http://pripareproject.eu/
EFFECTS+	Waterford Institute of Technology (IE)	€ 624K	5	http://www.effectsplus.eu/
SECCORD	Waterford Institute of Technology (IE)	€ 1M	8	http://www.seccord.eu/
TOTAL		€ 23M		

5

OTHER R&D PROJECTS



Other R&D Projects

Among the results that have the potential to lead to product innovation in ICT for citizens, the **biometric technologies** complementing traditional biometric recognition systems can be listed.

Complementary biometric technology provides a new and reliable solution for a **secure authentication** and can at the same time be used to provide an alternative way to access services by disabled people. In this domain the Call 1 **ACTIBIO** project has developed and piloted a car driver authentication model and has tested its biometrics technology recognizing system in the control rooms of a security company (Group4) and a transport company (Gotthard tunnel) with the goal to integrate biometric technologies in Ambient Intelligence security infrastructures. A similar approach to complementary biometrics for mobile devices has been followed by the **MOBIO** project (Call 1) focusing on the biometric authentication based on face and voice authentication in order to improve and integrate the conventional means of identification (passwords, secret codes and PINs).

From the combination between biometrics and cryptography **TURBINE** was funded by Call 1 to propose a multi-disciplinary privacy enhancing technology. Specific objectives of the project will be to ensure that the **crypto-protection** deployed on the biometric data is non-invertible and has the lowest possible impact on biometric verification performance. With similar purposes the Call 1 **PRIMELIFE** project (followed by **ABC4TRUST** in Call 5), has developed a theory and a technology for the privacy management of users based on anonymous digital credentials and encryption based on a web of trust. This result has received major media attention in the Netherlands (radio coverage, and a pilot live system with a sizeable number of users also thanks to the media coverage). This privacy-enhancing technique can also be used for virtual communities (social networks) and collaborative applications on the Internet.

The concept of **user centrality and identity management** is supported also by Call 1 **SWIFT** project, aiming at building a cross-layer user-centric identity framework for multitude of networks and services, supporting multiple personae.

Sensible **data management and processing** is the focus of **TAS3** project funded under Call 1, which aimed at developing and implementing an architecture with trusted services to manage and process distributed personal information. The project planned to focus an instantiation of this architecture in the employability and e-health sector allowing users and service providers in these two sectors to manage the lifelong generated personal employability and e-health information of the individuals involved. Another project developed a framework for controlling information exchange in composite Web services: the Call 5 **WEBSAND** framework consists of four major building blocks: a secure interaction model, methods for secure end-to-end information flow control, behavioral sandbox environments for secure client-side and server-side composition of multi-origin components, and a declarative and expressive policy description mechanism that ties the individual components together into a unified security architecture spanning client and server.

Many other funded projects have developed enhancing cyber security technologies, like 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.

Call 1 **AWISSENET** project for example, produced a toolbox to configure and support ad-hoc personal area networks and wireless sensor networks. It included intrusion detection, intruder identification and recovery based on distributed trust to provide security against malicious attacks. Network security is fostered also by the successful results achieved by **DEMONS** and **PRISM** (Call 1). **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. This project significantly advanced the ability to detect and respond

to large-scale threats while preserving citizens right to privacy, thus increasing societal acceptance of the need for being monitored.

A **privacy-preserving network monitoring system** has been developed by **PRISM** (Call 1) where carefully designed data protection mechanisms can coexist with suitably adapted monitoring applications. Ultimately, the goal of the project is to set a new de-facto standard for privacy-preserving traffic monitoring and deliver a tool that is guaranteed (and possibly certified) for legal compliance.

Standardization process is carried out also by **IN-SPIRE** project from Call 1, who aimed at developing traffic engineering algorithms, self-reconfigurable architectures and diagnosis and recovery techniques. The project also contributed to standardisation process in order to foster multi-operator interoperability and coordinated strategies for securing lifeline systems. Call 1 **INTERSECTION** project worked to enhance the European potential in the field of security by ensuring the protection of heterogeneous networks and infrastructures and contributed to standardisation process in order to foster multi-operator interoperability and coordinated strategies for securing networked systems. The Energy Sector Industry might also be considered a potential beneficiary for all projects which focus on infrastructural threats or attacks to controller devices in **critical infrastructures**, such as electricity meters. Projects SEC FUTUR, TWISNET and PINCETTE focused on these topics. **SEC FUTUR** (Call 5) worked on a **security engineering process for embedded system** including resource-efficient security building blocks and a framework for using those in the embedded system design supporting smart grid applications within advanced energy distribution and control infrastructures as well; **TWISNET** (Call 5) developed a platform for command and control over **wireless sensor networks** to be implemented into large scale industrial environments and enhanced with

privacy, confidentiality and reliability guarantees, designing protocols and architectures for interconnecting smart objects. Finally **PINCETTE** (Call 5) proposed a technology to ensure safe distributed infrastructure upgrades by validating continuously evolving networked software systems.

Trustworthiness of embedded systems is one of the targets of **SEPIA** (Call 5) project, whose purpose was to enhance security of mobile platforms, implementing cryptography and privacy protecting technologies, delta-evaluation and certification methodologies. SEPIA project aimed at **making embedded mobile platforms more secure** using process isolation and working on secure elements and operating systems, stressing at the same time the importance of a well-timed application of the certification, focusing on the reduction of the cost and time required for the certification processes.

A software certification method to fight against common security vulnerabilities is provided by Call 1 **SHIELDS** project. In order to achieve this objective SHIELDS partners developed novel formalisms for representing security information, such as known vulnerabilities, in a form directly usable by development tools, and accessible to software developers. This information will be stored in an internet-based **Security Vulnerabilities Repository Service** (SVRS) that facilitates fast dissemination of vulnerability information from security experts to software developers.

A systematic approach for development of trusted embedded systems including trust components in hardware, trusted operating systems based on secure virtualization, and trusted protocols has been developed by **TECOM** (Call 1), who in addition provided integrated packages for trusted operating systems, security layers, and trusted protocols, focusing on developers of embedded security-critical applications; it also studied and implemented some hardware solutions. ■

Community Building Activities

Projects Summary

Project	Coordinator	EU Contribution	Call	Website
ACTIBIO	CERTH (GR)	€ 3.2M	1	---
AWISSENET	CERTH (GR)	€ 2M	1	http://www.awissenet.eu
DEMONS	Telefonica I&D (ES)	€ 5.3M	5	http://fp7-demons.eu
INSPIRE	CINI (IT)	€ 2.4M	1	---
INTERSECTION	Elsag Datamat (Selex Elsag) (IT)	€ 2.9M	1	http://www.intersection-project.eu
MOBIO	IDIAP (CH)	€ 2.9M	1	http://www.mobioproject.org
PINCETTE	IBM (IL)	€ 2.8M	5	http://www.pincette-project.eu/
PRIMELIFE	ATOS (ES)	€ 10.2M	1	http://primelife.ercim.eu
PRISM	Telscom (CH)	€ 2.3M	1	http://www.fp7-prism.eu
SECFUTUR	SIT at Fraunhofer (DE)	€ 2.7	5	http://www.secfutur.eu
SEPIA	Graz University of Technology (A)	€ 2M	5	http://sepia-project.eu
SHIELDS	Linköping University (SE)	€ 3.2M	1	http://shields-project.eu
SWIFT	IAF at Fraunhofer (DE)	€ 1.8M	1	http://www.ist-swift.org
TAS3	Catholic University of Leuven (BE)	€ 9.4M	1	http://www.tas3.eu
TECOM	TECHNIKON (A)	€ 6.1M	1	http://www.tecom-project.eu
TURBINE	Sagem (Morpho) (FR)	€ 6.3M	1	http://www.turbine-project.org
TWISNET	Dresden Elektronik Ingenieurtechnik (DE)	€ 2.1M	5	http://www.twisnet.eu
WEBSAND	SAP (DE)	€ 3.2M	5	https://www.websand.eu
TOTAL:		€ 71M		

The following projects from Call1 and Call 5 are listed in the table below, since they never provided information on their future plans, nor achievements within the project. Only Cordis description is available.

Project	Coordinator	EU Contribution	Call	Website
AMBER	FCT at University of Coimbra (PT)	€ 1M	1	---
CONTRAIL	INRIA (FR)	€ 8.3M	5	http://contrail-project.eu/
ENDORSE	Waterford Institute of Technology (IE)	€ 2.7M	5	https://ict-endorse.eu
FORWARD	Vienna Technical University (AT)	€ 890K	1	http://www.ict-forward.eu
INCO TRUST	Waterford Institute of Technology (IE)	€ 830K	1	http://www.inco-trust.eu
INSTANT MOBILITY	Thales Services (FR)	€ 4.5M	5	http://www.instant-mobility.com
OPTIMIS	ATOS (ES)	€ 7.1M	5	http://www.optimis-project.eu/
PARSIFAL	ATOS (ES)	€ 600K	1	---
PASSIVE	University of Aegean (GR)	€ 2.3M	5	http://ict-passive.eu
PEACE	PDMFC Portugal (PT)	€ 2.6M	1	---
SERSCIS	University of Southampton (UK)	€ 2M	1	http://www.serscis.eu
TCLOUDS	TECHNIKON (AT)	€ 7.5M	5	http://www.tclouds-project.eu
VISION CLOUD	IBM (IL)	€ 9.1M	5	http://www.visioncloud.eu/
WOMBAT	Orange Labs - France Telecom (FR)	€ 2.8M	1	http://www.wombat-project.eu
TOTAL:		€ 53M		

CONCLUSION AND AFTERWORD

Conclusions

This handbook and the companion Success Stories booklet present the results of a comprehensive study on the innovation potential of ICT security, privacy and trust projects. It has been performed by the University of Trento, Italy, with the financial support of the EU Commission in the framework of the SECCORD FP7 Project. It is based on the analysis of public data and several interviews with project coordinators, technical and scientific leaders. Many of them went the extra mile to discuss and explain their results to us. This work would not have been possible without their commitment.

This document also aims to serve as a reference for the Trust & Security Programme projects. It outlines the key innovative results produced by its projects, shows how projects handle market acceptance gap for their technologies, and points out sources containing more detailed information about a project of interest.

As a whole, this handbook shows how far the H2020 overarching objective for the European DG CONNECT for Cybersecurity & Trust has been achieved in FP7, in the way of "fostering the industrial and technological resources required to benefit from the Digital Single Market", and thus

leading to the "emergence of a European industry and market for secure ICT" and "developing and adopting of industry-led security standards, technical norms and security-by-design and privacy-by-design principles by ICT product manufacturers and service providers".

These projects also show how a number of (sub) indicators for DG CONNECT in H2020 have been already achieved in FP7: spin-offs that directly market results of security research; ICT security solutions that are piloted close to a mass market affecting common citizens, and patent applications awarded in ICT security industrial technologies that follows from EU Funded research. They also demonstrate how the uptake of security solutions by lay users (public administrations, private companies, citizens) and the transfer of R&D results into ICT products and services are happening at an increasing pace.

In summary, many European research projects in ICT Security and Trust have been particularly successful in shortening the gap from research to innovation and thus creating the stepping stone for a vibrant market in secure and trustworthy ICT in Europe. ■

Afterword

Moving from FP7 to Horizon 2020

As this handbook shows, the numerous projects in the field of Trust and Security funded under FP7 address not only fundamental research but also the economic and societal dimension of security and privacy in the digital ecosystem. Over 7 years, several calls with their topics allowed European scientists and researchers to progress on providing solutions to issues that are still emerging and constantly developing. If you compare 2007, the start date of FP7, with 2015 you will have noticed that the digital world has changed enormously and this applies also for cybersecurity and online privacy. Digital security is a more and more multi-faceted issue involving critical economic and civilian stakes, cybercrime, online privacy and the protection of fundamental rights. Research today in this area must address security, trust and privacy coherently from all perspectives (technological, economic, legal and social). It is also strongly linked to the promotion of innovation and economic growth in the EU, while protecting Europe's society, economy, assets and fundamental rights. Therefore, the change from FP7 to Horizon 2020 is very much welcome. As Vice-President Commissioner Neelie Kroes has highlighted in February 2014 "It strengthens our investment in cyber security, privacy and trustworthy ICT. We already have strong capacity in areas like business software, smart cards, and cryptography: now we can build on that."

Horizon 2020 has introduced several innovative new instruments that allow us to target our research and innovation policies in digital security better to the impacts intended. Innovation Actions, the SME instrument and pre-commercial procurement are new ways to support innovative European companies and researchers to reach the markets with their new products and services, enabling European industry in IT-security to become more competitive and reach high European standards in cybersecurity and online privacy.

At the same time, Horizon 2020 allows the European Commission to continue its support to address fundamental research questions, for in-

stance for new approaches in cryptography and to help defining and applying the concepts of security-by-design as well as privacy-by-design. These ambitions are now being implemented in Horizon 2020. First calls took place in 2014 and over the last months the first projects have been launched. It will be very interesting to watch them carefully with FP7 in mind in order to identify the benefits of the new Horizon 2020 approaches and hopefully an even higher number of success stories.

Horizon 2020 is a comprehensive framework for Research, Development and Innovation in the field of Digital Security. It addresses the objectives in mainly two streams:

- Leadership in enabling and industrial technologies (LEIT): Cybersecurity, Trustworthy ICT
- Societal Challenges 7: "Secure societies – Protecting freedom and security of Europe and its citizens"

However, these funding streams will only cover parts of the digital security area. In many other streams you will be able to identify calls directed as research and innovation topics strongly related to cybersecurity and online privacy. In LEIT this might be Internet of Things (IoT), Cloud Computing, Big Data and others. In Societal Challenges this could be found in calls related to eHealth, Smart Cities, Automated Transport or Energy Efficiency. And then there are calls in Future Emerging Technologies, joined calls with third countries or calls directed at SMEs, which are not specific to topics like digital security, but could be very attractive alternatives.

We are aware that in particular initial phase of Horizon 2020 might be complicated to stakeholders, who are used to FP7 and its predecessors, but we strongly believe to be now better equipped to meet the EU's goals for a trustworthy digital society. Our team is very dedicated to support you in finding the best available funding in Horizon 2020.

To focus the EU's research funding in the most efficient manner and to best identify challenges and opportunities in the field, close collaboration with all stakeholders is primordial.

For this aim, the public-private Network and Information Security Platform (NISIP) was established in June 2013, as part of the EU Cybersecurity Strategy. The Platform counts over 200 organisations¹ as its members, who so far have gathered for several plenary meetings, and many more telephone conferences, over the almost two years of its existence. This work is a good beginning in a process that aims to build trust and security over the long and diverse value chain linking together providers and users in the European digital marketplace.

The NIS Platform is also working on Strategic Research Agenda for secure ICT, which will serve as a key input to the European Research and Innovation agenda and will be the major building block for defining the European Commission's approach for the remainder of Horizon 2020 and possibly beyond 2020.

Among others, a key focus of the research agenda will be on turning research results into commercial products, to serve Europe's growth and jobs objectives and in this the European Commission's support in Horizon 2020 is closely related to the "Cybersecurity Strategy of the European Union – An Open, Safe and Secure Cyberspace", which also aims at fostering the industrial and technological resources required to benefit from

the Digital Single Market to stimulate the emergence of a European industry and market for secure ICT and the growth and competitiveness of the EU economy. Finally, all this should also increase the public and private spending on cybersecurity Research and Development (R&D) in Europe, rendering it a global leader in cybersecurity and online privacy.

All this can only be achieved with the help of European researchers, academics, enterprises, which are ready to dedicate their careers to further digital security and also to take the risk for proposing new ideas, concepts and products. We in the European Commission are very much looking forward to work with you in Horizon 2020 and to be able to tell some exciting stories about in seven years' time. ■

Martin Mühleck
ICT Trust and Security -
Programme Officer





**SECCORD / Security and Trust Coordination
and Enhanced Collaboration**

Contact Info

 **Prof. Fabio Massacci**
Università degli Studi di Trento
 **seccord@unitn.it**

www.seccord.eu