UNIVERSITÀ DEGLI STUDI
DI TRENTO

SecCord

SUCCESS
STORIES

Success Stories of FP7 ICT Trust & Security Projects

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

Foreword by Jakub Boratynski
Head of Unit of Trust and Security, DG CONNECT, European Commission

Success Stories
FP7 ICT Trust & Security Projects
Version I, March 2015

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

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

This document is the **Annex 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 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 a selection of success stories based on available information and to present them in this brochure. It provides valuable insights and is representative of the research carried out by EU-funded projects in the field since 2007. European scientists and companies are working hard to make the journey to a trustworthy digital world. I invite you to read this overview and join them in their effort so Europe can fully benefit from the exciting opportunities in front of us. ■

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

Success Stories Highlights

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"?

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".

From a technical perspective, all research projects funded by the EU Commission have undergone a technical 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 European 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**.

This short report and the companion handbook report 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.

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: the creation of a spin-off company to finalize and commercialize the results of the project, the internal follow-up with new human resources assigned by a company to the further development and commercialization of the product, the incorporation in whole or in part of the actual technology in a product or a production process, the creation of valuable intellectual property worth patent protection.

A different, but equally valuable direction, is the general contribution to a more secure digital ecosystem. In this realm we can include the adoption by other companies and citizens of the specific research results leading to a safer internet, the contribution to world-wide standards on secure and privacy-preserving technologies, 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 going outside university and industry laboratories. From this perspective we can also classify as success stories projects that piloted their technologies with citizens and end users either by making them available on the web or by directly engaging with citizens.

Not all research projects are at the same state of development and this must be necessarily reflected in the assessment: some projects were funded at the beginning of the FP7 Framework programme and ended several years ago; others funded at Call 10, one of the last calls, are still hammering their research results into shape. For the purpose of this study, projects have been thus clustered in four groups:

1. **12 Success Stories in ICT Security and Trust** according to the above mentioned criteria. These projects have been funded with 49 million euro, 14% of the total EU budget spent in FP7 ICT security and trust (361 million euro);
2. **19 Innovative projects working towards the market** which are reaching maturity, validating their results through different means (pilots, testbeds, experiments) and might become

success stories at some point. They account for 80 million euro, namely 22% of the total EU budget of the area;

3. **18 Technical successful projects** which presented their technical achievements but did not have compelling evidence on their road towards a digital market (85 million euro and 23% of the total);
4. **Community Building Activities** (Coordination and Support Actions and Network of Excellence) aim at providing effective, practical and useful means of communications, coordination, networking and dissemination. Under these funding schemes **17 projects** have been supported, for a little less than 23 million euro, 6% of the total;
5. There are **32 Other R&D projects** which did not reply to requests of sharing and discussing the innovation potential of their technical results (124 mIllion euro and 34% of the total).

This booklet showcases 12 success stories. Additional details, such as project contacts and the overall list of projects can be found in the companion FP7 Security and Trust handbook.

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 several rounds of significant funding to essentially the same consortium. 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.

The European Commission funding of 361 million euro pales against the investment of venture capital in ICT security: according to data collected by Thomson Reuters [1], venture investors put nearly $3 billion into cyber security companies between 2011 and 2013, resulting in new funding for some 300 firms.

According to Forbes research [2], only one in 10,000 funded startups end up being worth over $1 billion. 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 around 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.

The projects in this booklet are the pioneers of future digital market in ICT. ■

Martina de Gramatica
Fabio Massacci

[1] http://www.darkreading.com/venture-capital-the-lifeblood-behind-security-innovation/d/d-id/1234834
[2] http://www.forbes.com/sites/petercohan/2014/01/03/will-venture-capital-beat-the-market-in-2014/

Success of European crypto-teams

CACE
Computer Aided Cryptography Engineering

Call 1 — 36 months

12 Partners

€ 3.5M EU Contribution

www **http://www.cace-project.eu**

Today cryptography has become an essential tool to protect confidentiality and integrity of sensitive data. It is used virtually everywhere – from microcomputers and embedded systems to Cloud services. The main advantage of cryptography-based protection is that it is backed up by formal proofs of security.

Europe has a scientific leadership in research and development in cryptography and several organizations in Europe are worldwide known for excellence in this field. The presence of University of Bristol (UK), Aarhus University (Denmark) and Barl Ilan University (Israel) contributed to the successful results achieved by the Call 1 CACE project.

Started in 2008 and ended in 2010, CACE was dedicated to the development of a toolbox to support a high quality cryptographic software design. The proposed toolkit will allow non-experts to develop high-level cryptographic applications and business models by means of cryptography-aware high level programming languages and compilers.

Many partners in CACE have exploited the results of the project. Just four years after its end, two start-ups brought their solutions to the market on the basis of the CACE achievements: Partisia [3] (a spin-off of Aarhus University) offers a secure auction-as-a-service), and Dyadic Security [4] (a spin-off of University of Bristol and Bar Ilan University) offers a technology to store cryptographic keys in a distributed way, thus removing a compromised server as a single point of failure. These start-ups develop their technologies to a new level in the framework of the PRACTICE project (Call 10).

Nokia, another partner, has exploited the CACE results in its products: now Nokia phones run 256 bit Elliptic Prime Curve implementation by the CACE tools. ■

Using Data in the Cloud without Surrender

SECURESCM
Secure Supply Chain Management

Call 5 — 36 months

4 Partners

€ 2.1M EU Contribution

www **http://www.securescm.org**

Secure multi-party computation is a technology that allows several parties to contribute data to compute a particular result without revealing the actual data of each partner. The data is encrypted, and the joint computation is executed using cryptographic protocols designed to compute on encrypted data. For example, a number of companies involved in a joint supply chain can use encrypted data of partners to plan logistics and execute supply chain management. Even more challenging example is secure benchmarking, when companies can submit their key performance indicators encrypted to the cloud and use the competitors' statistics to evaluate their own performance.

The SECURESCM project (starting within Call 1) delivered secure multi-party computation protocols for supply chain management in the cloud, including supply chain profit maximization on private data. This secure multi-party computation technology will definitely allow European companies to collaborate more efficiently while not surrendering their private data to business partners and the cloud service provider.

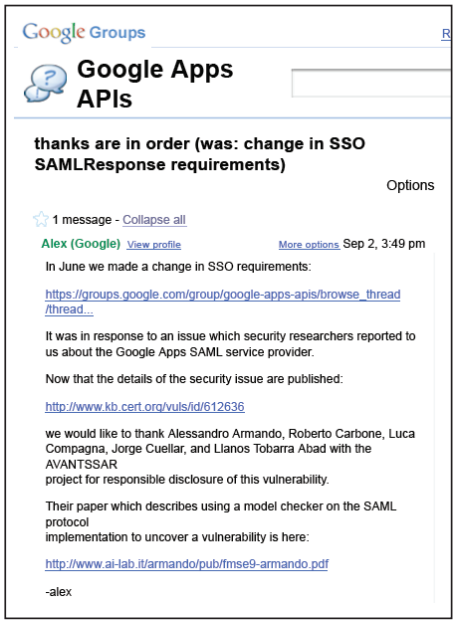
The intellectual property developed as part of SecureSCM led to several patent applications in secure collaborative supply chain management generating a leading position for the world's largest business software manufacturer SAP. SAP also ran an entrepreneurial effort to establish a new product as part 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. In the current years the project has been continuing the investment to help cloud customers staying in control of their data, fostering a Customer-Controlled Security in the Cloud. The project did not originally aimed for it, but clearly emerged that this was "the" topic. It is also planned to integrate it into the SAP flagship product HANA.

The successful results achieved by the SecureSCM project led to a direct employment raise at SAP. the project funded slightly more than a full time equivalent researcher; to develop the pre-commercial version, 6 people have been employed full time for two years after SecureSCM was completed. ■

[3] http://www.partisia.dk/pages/default.aspx
[4] https://www.dyadicsec.com/

Kudos from Millions of Businesses

Google reports that 5 million businesses (including a vast number of SMEs) use Google Apps to implement their essential business services. Google Apps also enable creation of federated environments where each end-user can use his credentials to access not only apps of its own company, but also apps of business partners. This is called the Single-Sign-On (SSO) mechanism.


Google Groups

Google Apps APIs

thanks are in order (was: change in SSO SAMLResponse requirements)

Options

1 message - Collapse all

Alex (Google) View profile More options Sep 2, 3:49 pm

In June we made a change in SSO requirements:

https://groups.google.com/group/google-apps-apis/browse_thread/thread...

It was in response to an issue which security researchers reported to us about the Google Apps SAML service provider.

Now that the details of the security issue are published:

http://www.kb.cert.org/vuls/id/612636

we would like to thank Alessandro Armando, Roberto Carbone, Luca Compagna, Jorge Cuellar, and Llanos Tobarra Abad with the AVANTSSAR
project for responsible disclosure of this vulnerability.

Their paper which describes using a model checker on the SAML protocol
implementation to uncover a vulnerability is here:

http://www.ai-lab.it/armando/pub/fmse9-armando.pdf

-alex

Google acknowledges AVANTSSAR contribution

SSO works by enabling an exchange of authentication and authorization information across multiple independent systems. With SSO a user needs to log in only once with an identity provider, and is not prompted for logging in with each individual system (a service). Security Assertion Markup Language (SAML) is a standard of data format for SSO. Google has implemented a SAML-based SSO protocol for Google Apps.

What can happen if SSO is not secure? If a malicious company can get access to the actual credentials of the end-user, or some authentication data, then it can spy on other enterprises in the federated environment.

The **AVANTSSAR** project (Call 1) has studied the open source Google's implementation of SSO and formalized it in the ASLan++ language developed by AVANTSSAR. The formal specification was then analyzed with the AVANTSSAR platform, and bugs were revealed, that could have affected operations of millions of Google Apps customers. The first discovered bug was enabling a crude man-in-the-middle attack, when a malicious service provider could access all user accounts in a federated environment, if the users were previously authenticated with him. This is exactly the scenario we discussed above.

Google has rolled out updates for Google Apps fixing the vulnerabilities. Later AVANTSSAR has discovered more bugs in other SAML implementations, as well as a bug in the SAML SSO use case described in the SAML Technical Overview. Based on their experience, the project participants conclude that similar vulnerabilities are most probably present in other proprietary implementations of SSO. Google and its SME users were not members of AVANTSSAR. Yet, they greatly benefitted from these technologies. Several other companies can benefit as well by using AVANTSSAR formal verification tools. ■

AVANTSSAR

Automated Validation of Trust and Security of Service-oriented Architectures

Call 1 — 36 months

10 Partners

€ 3.8M EU Contribution

http://www.avantssar.eu

A new generation of analyzers for automated security validation

Innovative products for ICT specialists in security certification, verification and testing are delivered by the Call 5 project **SPACIOS**, born as AVANTSSAR project follow-up. In its project life, SPACIOS developed a set of techniques for property-driven security testing, and a set of techniques for vulnerability-driven testing, where tests or test strategies are derived from vulnerabilities (e.g., XSS) likely to invalidating the security goals. Lastly the project also fostered 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.

These techniques have all been implemented and integrated into the SPACIOS Tool. The tool as a proof of concept has been applied on a set of security testing problem cases drawn from industrial and open-source IoS application scenarios, thereby paving the way to transferring project re-

SPaCIoS

Secure Provision and Consumption in the Internet of Services

Call 5 — 40 months

9 Partners

€ 3.6M EU Contribution

http://www.spacios.eu

sults successfully to industrial practice and to standardization bodies and open-source communities.

Some of the research outcomes have been applied in various consultancy initiatives at SAP and SIEMENS. For instance, the model-based testing approach has been used to verify and test security standards under development, at that time, at SAP (e.g., SAP OAuth2 for the ABAP application server). Following up the results obtained in SPACIOS, SAP has started an internal project. Furthermore, a security testing engine prototype, borrowing techniques and know-how from SPACIOS (e.g., the VERA engine), has been introduced within the SAP Web IDE, a web based tool designed for developers to rapidly design, build, and deploy SAP Fiori-like web applications based on SAPUI5 for desktop and mobile devices [5].

This project is still in-progress, but initial features are already available for piloting end users of SAP Hana Cloud. Within the project 4 patents have been filed. ■

Trusted Biometrics solutions

Among the results with the potential to reach a product innovation in ICT for citizens, biometric technologies complementing traditional biometrics (such as fingerprints or iris recognition) can be listed. Several projects have been working in order to develop and improve effective countermeasures against attacks and vulnerabilities, increasing the reliability and the trustworthiness of the biometric systems.

One of these projects succeeded in producing a marketable solution that has been taken up by an interested company. **TABULA RASA** project responded to the Call 5 with the aim to propose reliable countermeasures against spoofing attacks to biometric systems. The project expected to create jobs within the European SME sector as its results are integrated into commercialised solutions. For example, the Swiss based start-up KeyLemon [6] has integrated into a final product the face recognition software countermeasure developed by TABULA RASA. The expertise developed by this project helped KeyLemon to secure a series A investment of $1.5M, creating several jobs within the company.

In a similar way, Morpho (Safran), the world leader in biometric solutions, is also deeply involved, bringing its invaluable expertise and market vision to the consortium.

Ryan Heath, former- European Commission spokesman for the Digital Agenda and Digital Technologies stated: "*Many of us keep personal and confidential information on our smartphones and tablets, so we need to have confidence that we can fully rely on these biometric tools. The European Commission is pleased with TABULA RASA's success so far. No other research group has achieved such advanced results in biometrics to date*".

The successful achievements of TABULA RASA project are partially based on the MOBIO results (Call 1) and paved the way for a sister FP7 project, BEAT (Biometric Evaluation and Testing), aiming at creating a set of industry guidelines for assessing biometric security performances. ■

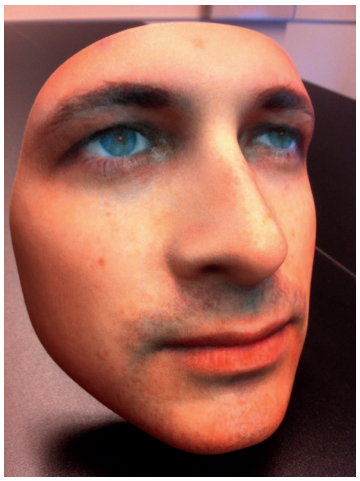
TABULA RASA
Trusted Biometrics under Spoofing Attacks

Call 5 — 42 months

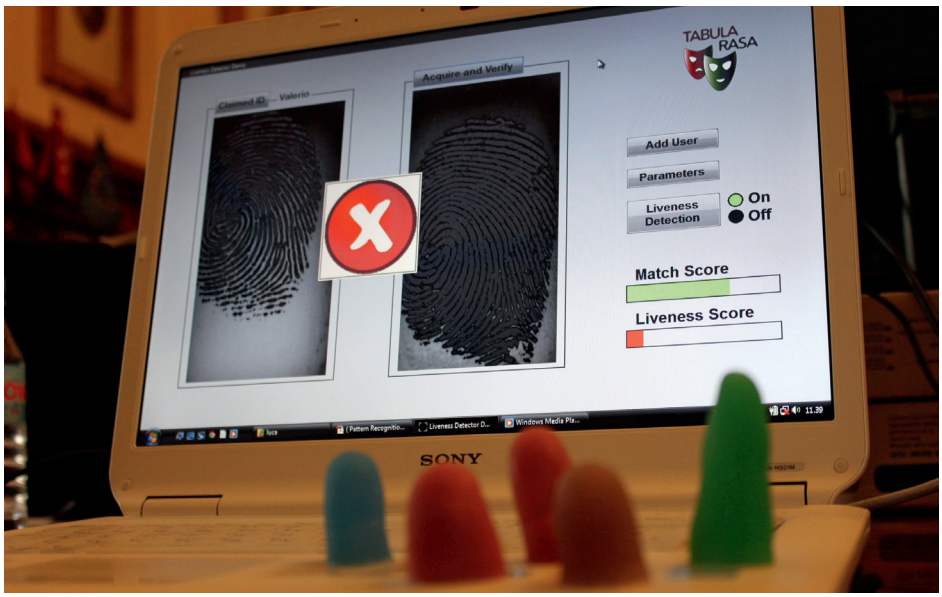
7 Partners

€ 4M EU Contribution

http://www.tabularasa-euproject.org



A custom-made life size mask ordered over the Internet.



Fingers used for the demonstration of TABULA RASA fingerprints recognition system.

[5] https://help.hana.ondemand.com/SAP_RDE/frameset.htm?0221845d73ad403ab2852142f3179177.html
[6] https://www.keylemon.com/dev/tag/biometric/

A secure Data Sharing

Data sharing is a key element of any cross-organizational supply chain; nevertheless, most of the organizations involved in such supply chains worry about security of data exchange. Therefore it is crucial to ensure that all interactions and data sharing happen in accordance with some well-defined and automatically manageable policies.

The **CONSEQUENCE** project (funded by Call 1, started in 2008 and ended in 2010) has developed a Data Sharing Agreement (DSA) Authoring Tool. As stated by Matteucci et al. "*A Data Sharing Agreement (DSA) represents a flexible means to assure privacy and security of electronic data exchange. DSA is a formal document regulating data exchange in a controlled manner, by defining a set of policies specifying what parties are allowed, or required, or denied to do with respect to data covered by the agreement*" [7].

The developed tool allows to formally express data sharing agreements in a special language CNL4DSA, supporting policies for data access authorization, obligation and prohibition. The technology has been patented by Hewlett-Packard Development Company, a partner in the CONSEQUENCE consortium. Two additional applications of the CONSEQUENCE project in the area of complex authorizations (for *enforcing* data-sharing policies) were awarded with patents. ■

CONSEQUENCE
Context-aware Data-centric Information Sharing

Call 1 — 36 months

7 Partners

€ 2.9M EU Contribution

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

Don't be infected: A public service for citizens to secure their computers

Many citizens today are concerned about their personal computer security and protection while surfing the Internet. They are afraid that their PC can be infected with malware, and their sensitive data, like passwords or credit card numbers, might get in the hands of cyber criminals, or that their device becomes a part of a botnet. However, even more citizens are not aware of cyber threats. With the sophisticated malicious threats present today, both aware and not aware citizens might become victims. Yet, if the user is aware it is more attentive to what it does on the Internet, and can notice problems earlier.

The **ACDC** project has been funded from Call 8 under the CIP (Competitiveness and Innovation Framework Programme) with a short time to market. It focuses on pilots for fighting botnets, by deploying already identified research technology.

After one year of operation it has already opened a dedicated online service for European citizens to inform them about cyber threats and botnets, and to help them check their devices for malware, and protect the devices against new threats.

The service is publicly available [8]; it contains dedicated pages for information about botnets, a step-by-step manual and a list of tools for cleaning the personal computer from malware and prevention from future infections. Note that this service can be useful not only for citizens but for organizations as well, as the project has prepared also a list of products that are suitable for enterprise environments. This information can be especially valuable for SMEs. ■

ACDC
Advanced Cyber Defence Centre

Call CIP 8 — 30 months

28 Partners

€ 7.7M EU Contribution

http://www.acdc-project.eu

Towards a uniform security environment

«*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*

[7] http://wafi.iit.cnr.it/sites/default/files/DPM11-final.pdf

[8] https://www.botfrei.de/en/index.html.

SECURED
SECURity at the network Edge

Call 10 — 36 months

7 Partners

€ 2.7M EU Contribution

www **https://www.secured-fp7.eu/**

HINT
Holistic Approaches or Integrity of ICT-Systems

Call 8 — 36 months

7 Partners

€ 3.4M EU Contribution

www **http://www.hint-project.eu**

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, Politecnico di Torino.

In order to protect users from network threats, the Call 10 **SECURED** project aims at 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/his devices and have it applied automatically at the point where she/he connects to the network.

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.

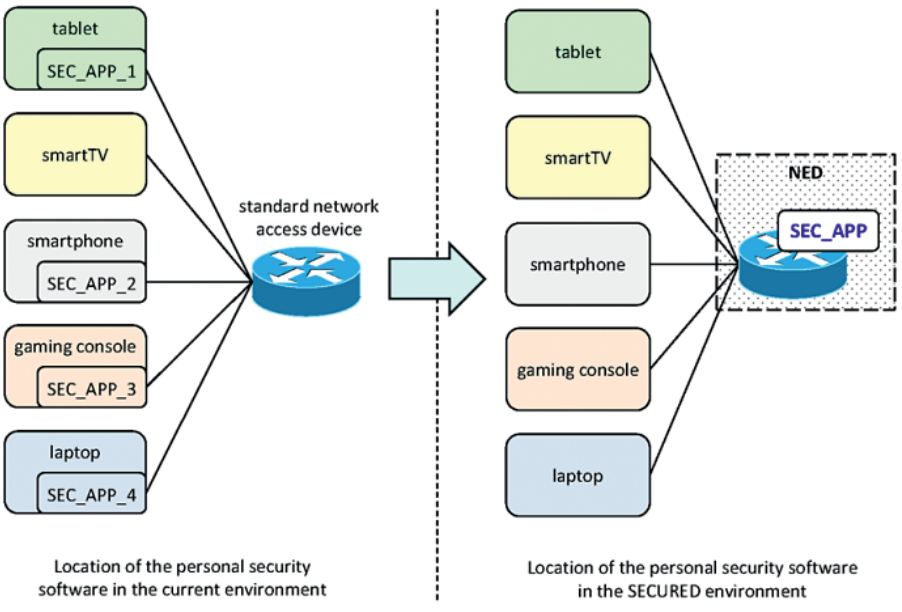
In order to validate its results, the project will run two pilots in the coming years: one pilot focusing on the home gateway scenario (managed by the SECURED partner PrimeTel and involving its actual subscribers as real end-users), and another pilot based on the corporate security scenario run by VTT. The pilots will involve about 100 real users by the end of the project.

Many are the innovation achievements planned by this project so far; SECURED aims at working on the architecture of a programmable device to host the security applications off-loaded from the end-user terminal; a set of protocols to interact with and an implementation of this programmable device, and a mechanism to simplify definition and application of the user's security policies for the applications run at the SECURED device.

On the side of the hardware security, the **HINT** project (funded under the Call 8) 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. In order to illustrate the use of those technologies in real-life products, two demonstrators are currently being implemented in two respective case studies: an embedded PUF structure is used for providing digital signature in a practical ID smart card-based scenario (led by Morpho company); and a HT detection demonstrator based on the platform used in a Professional Mobile Radio (PMR) terminals is played in an industry-oriented scenario (led by Cassidian Cybersecurity, a major manufacturer of PMRs in Europe).

Two patents have been filed so far by two of the project partners. The partners of the HINT consortium are also currently laying the foundations for a new ISO standard for the PUF technology.

Embedded systems requiring particularly enhanced security levels are those related to critical infrastructures (CI). In the last years indeed, it became apparent that CI is not only at risk from natural disasters but might also be attacked by malicious individuals, as Stuxnet inci-



Moving security applications from user terminals to the network (network edge device (NED)) - HINT

dent demonstrated for instance. The Call 1 **WSAN4CIP** project started in 2009 and 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. The project 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. 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 one successful contribution to IETF standardization. ■

WSAN4CIP
Wireless Sensor and Actuator Networks for Critical Infrastructure Protection

Call 1 — 36 months

6 Partners

€ 2.8M EU Contribution

http://www.wsan4cip.eu

Citizens' privacy matters: results from user trials

«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 a new element: it is up to the user to uncover the elements of his/her identity that he/she really wants to release to the service, or to uncover only the parts of his/her identity needed for the service. So the innovation will be mainly the empowerment of the user, so that his e-Identity is in his hand» Yannis Stamatiou, Diophantus – Computer Technology Institute & Press.

ABC4Trust (Call 5 - started in 2010, ended in 2015) worked on privacy-enhancing Attribute-based Credentials (Privacy-ABCs). It can be seen as a follow-up of the FP6 PRIME project and the FP7 PrimeLife project. 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 regains control over their personal data.

The project conducted two pilot trials, whose results were evaluated in spring 2014.

ABC4Trust set up a privacy-preserving communication network in a Swedish school. 55 school personnel, 123 pupils and 203 parents – with a total of 381 people – were actively involved in the Norrtullskolan School of Soederhamn to take part to the pilot. Compared to other social networks, the

ABC4TRUST
Attribute-based Credentials for Trust

Call 5 — 52 months

12 Partners

€ 8.8M EU Contribution

https://abc4trust.eu/

Swedish pupils using the ABC4Trust-enabled social network

PICOS

Privacy and identity management for community services

Call 1 **41 months**

10 Partners

€ 4.0M EU Contribution

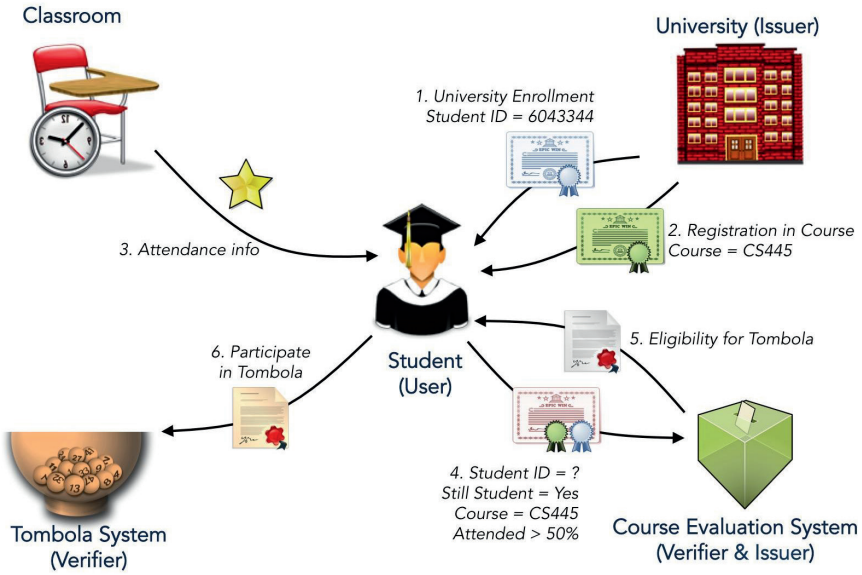
http://www.picos-project.eu

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. An anonymous questionnaire circulated after the trial shows that the target group understood the objective of the project and the concept of Privacy-ABCs. A large majority of the target group also clearly expressed a high interest in being informed about which personal data they reveal and how they can control it.

ABC4Trust also implemented a course evaluation system at a Greek university. Around 100 students were involved in two rounds; the students were enabled to evaluate their courses anonymously, while the system guaranteed that only duly accredited students who had visited a minimum number of lectures 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.

gotiations are underway to integrate the pilots into larger systems and regular use. So in the not so far future we expect more European public services and other organisations to switch to Privacy-ABCs" states the coordinator of the project, Prof. Dr. Kai Rannenberg from Goethe University Frankfurt.

Another project who put considerable effort in running pilots with real end users is **PICOS** from Call 1. 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. The designed pilots involved two different communities: anglers and on-line gamers. The first trials were conducted between November 2009 and May 2010 with 24 anglers in two groups in Vienna and Kiel. Then 25 on-line gamers participated in Vienna and Brno. All 49 users have been observed and interviewed to gather the results. The results aimed at directing the improvements which have to be developed before bringing the prototype into a real-world context. Within the second trial with the members of an online community, a group discussion and a scenario-based evaluation of the PICOS concepts was added to gather feedback on the privacy enhanced technology features which were



Architecture of the ABC4Trust framework for a Greek university

In summary, implementing ABC technology requires a rethinking of authentication and data exchange processes, as we know them. Though the cryptographic technology of Privacy-ABCs was known before, ABC4Trust has contributed (and will keep on contributing) towards the actual usage of the technology. To this extent the project has contributed to several ISO/IEC standards.

"*The respective authorities are happy with the pilots and the feedback. Active ne-*

briefly introduced. During the lab test the participants were observed and interviewed during they solved several tasks and questions regarding these tasks have been afterwards administered via an online questionnaire.

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. ■

Success Stories Overview

Project	Participating Countries	Website	Call	Duration	EU Contribution
ABC4TRUST	Belgium, Denmark, France, Germany, Greece, Sweden, Switzerland	https://abc4trust.eu/	5	52 months	€ 8.8M
ACDC	Austria, Belgium, Bulgaria, Czech Republic, France, Germany, Hungary, Italy, Netherlands, Portugal, Romania, Slovenia, Spain, United Kingdom	http://www.acdc-project.eu	8	30 months	€ 7.7M
AVANTSSAR	France, Germany, Italy, Romania, Switzerland	http://www.avantssar.eu	1	36 months	€ 3.8M
CACE	Austria, Denmark, Finland, Germany, Israel, Netherlands, Portugal, Switzerland, United Kingdom	http://www.cace-project.eu	1	36 months	€ 3.5M
CONSEQUENCE	Germany, Italy, United Kingdom	http://www.consequence-project.eu/	1	36 months	€ 2.9M
HINT	Austria, Belgium, France, Germany	http://www.hint-project.eu	8	36 months	€ 3.4M
PICOS	Austria, Belgium, Czech Republic, Germany, Spain, United Kingdom	http://www.picos-project.eu	1	41 months	€ 4.0M
SECURED	Cyprus, Finland, Italy, Spain, United Kingdom	https://www.secured-fp7.eu/	10	36 months	€ 2.7M
SecureSCM	Germany, Italy, Netherlands, Spain	http://www.securescm.org	5	36 months	€ 2.1M
SPACIOS	France, Germany, Italy, Romania, Switzerland	http://www.spacios.eu	5	40 months	€ 3.6M
TABULA RASA	China, Finland, France, Italy, Spain, Switzerland, United Kingdom	http://www.tabularasa-euproject.org	5	42 months	€ 4.0M
WSAN4CIP	France, Germany, Portugal, Hungary, Spain, Sweden	http://www.wsan4cip.eu	1	36 months	€ 2.8M

Conclusions

This short report and the companion handbook 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. ■

For more information please have a look at the overall FP7 T&S Projects Handbook available at www.seccord.eu

SecCord

SECCORD / Security and Trust Coordination and Enhanced Collaboration

Contact Info

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

www.seccord.eu