UNIVERSITÀ DEGLI STUDI
DI TRENTO

SecCord

YEARBOOK 2014

FP7 Security and Trust Research Projects

M. de Gramatica, O. Gadyatskaya, F. Massacci, A. Pasquali
Univerity of Trento, July 2014

SEVENTH FRAMEWORK
PROGRAMME

Opinions expressed here are not necessarily endorsed by the European Commission and by the projects described in this document. 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.

Department of Information Engineering and Computer Science
University of Trento
Prof. Fabio Massacci - fabio.massacci@unitn.it
Via Sommarive 5, 38123 Trento, Italy
tel: +39.0461.282086
fax: +39.0461.282093
https://securitylab.disi.unitn.it/

This document is the Annex B of D 3.2 “Research and Innovation Yearbook 2014” for the SecCord Project.
The research leading to these results has received funding from the European Union Seventh Framework Programme (FP7/2007-2013) under grant agreement n° 316622 SECCORD.

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

Executive Summary

The aim of this second Yearbook is to provide a comprehensive description of the R&D projects executed under the Trust & Security Programme and to present the discoveries of the study conducted with the project leaders involved. **The Yearbook aims to provide key stakeholders a picture as complete as possible on the key results achieved by the projects in terms of innovations and the planned strategies to overcome the constraints of the market**.
The 2014 Yearbook follows the same approach to investigation used for the 2013 Yearbook: it moves along with the projects themselves, trying to report in a systematic way the evolution of results, changes, problems and solutions which projects members encounter during the life-cycle of the projects.

As the European Commission already produces a number of statistical reports we have chosen a qualitative research approach and collect data through a series of structured interviews with project leaders. We managed to conduct the interviews vis-à--vis during project's events, workshops and conferences whenever possible, otherwise via telephone calls or Skype calls. Also in this occasion -- as in previous years -- events such as the CSP EU Forum proved once again to be a fruitful chance to get in touch with other projects members, sharing information and creating potential working relationships for the future.

This document presents in total 32 projects from the Call 1, Call 5, Call 8 and Call 10. They offer a good overview of the FP7 Framework's landscape for R&D in Security and Trust as they are captured at different points of a project's lifetime. Projects launched in Call 1 and the Joint ICT-SEC Call have completed several years ago; projects executed in Call 5 and the ICT-FI Call have just completed their activities in the past year; projects selected in Call 8 are in their second year-life year, while Call 10 projects have just started last year. Some projects did not respond to our requests and therefore they are not reported.

We present at first a **summary of the analysis and provide a synthesis of our stakeholders' opinion on the ICT Security market in Europe, its strength and its weaknesses. We discuss the threat and opportunities for market players and how they are validating their research results in order to meet these market needs. Further we investigate what could be promising avenues of research in ICT security according the project leaders**.

Then we report the actual results of the individual projects as follows:

- The first group of projects is composed by what we can rightly define as **Success Stories**. A small range of 4 projects have been selected as they 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. We focus in particular on Call 1 projects that at the end of their like-cycle project had produced two start-ups bringing their solutions into the market (CACE) and released a world-wide patent on Data Sharing Agreement Authoring (CONSEQUENCE). A positive example of piloting with real end users was provided by a Call 5 project, ABC4TRUST, that tested its results on school pupils and university students. Finally, a CIP (Competitiveness and Innovation Framework Programme) Call 8 project, ACDC, is presented. It deployed a dedicated online service for European citizens to inform them about cyber threats and botnets, helping them check their devices for malware, and protect the devices against new threats.

- Projects from Call 8 offer a chance to focus into the **Recent Developments** they delivered last year, when we interviewed them as Discovery projects, just started. Now they are reaching maturity, validating their results through different means (pilots, testbeds, experiments) and approaching to the market arena, occasionally bumping into challenging gaps.

- We grouped in the **Innovation Project Highlights** those projects from Call 5, 8 and 10 that we never had the chance to interview beforehand with the aim to have a look into what their objectives are and how they are planning to produce innovation for the market.

- The last section ends with **Coordination and Support Actions** projects, which aims 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.

After this study, we believe that the FP7 R&D projects in security and Trust have delivered a significant number of important research results. This Security and Trust Yearbook for 2014 should capture the best of this collective effort. ■

1.1 SUCCESS STORIES

A minimal disclosure technology

ABC4TRUST

Attribute-Based Credentials for Trust

Coordinator
Johann Wolfgang Goethe University Frankfurt (DE)

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

Dates
2010-11-01 to 2014-10-31
Participants Number
12
Website
https://abc4trust.eu/
Classification in CORDIS
Collaborative project
Call
5
Budget
€ 13.585.497

«One of the possible innovations resulting from this project is to introduce a new e-Identity concepts and new e-Identity management techniques. The focus will be 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 hand».
Yannis Stamatiou - University of Patras

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.

INNOVATION ACHIEVEMENTS

Another important factor for the usage of Privacy-ABCs is standardisation. ABC4Trust is participating in ISO/IEC standardisation (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

While the pilots were employing smart cards and smart card readers as hardware devices, it is also possible to use Privacy-ABCs on mobile devices. ABC4Trust presented the research results on this field at several conference.

PILOTS

ABC4Trust set up a privacy-preserving communication network in a Swedish school. 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.
ABC4Trust also implemented a course evaluation system at a 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.

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 centes.
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 where Telecom Italia in involed, Belgium with LSEC participation and Croatia through CARNet Service contribution ; and also public cyber security services for citizens.

Coordinator
ECO - Association of the German Internet Industry, Germany

Participants
ATOS Spain, Barcelona Digital Spain, Bulgarian Posts Bulgaria, Cassidian Cybersecurity France, Cognitive Security Czech Republic, CARNet Croatia, CyberDefcon, DFN-CERT Germany, DE-CIX Germany, Telecom Italia Italy, ENGINEERING Italy, FCCN Portugal, FKIE of Fraunhofer Germany, G Data Software Germany, Institute for Internet Security Germany, Inteco Spain, ISCOM Italy, Catholic University of Leuven Belgium, LSEC Belgium, Microsoft EMEA France, Montimage France, CERT-RO Romania, SignalSpam France, TECHNIKON Austria, Telefonica I&D Spain, Technical University of Delft Netherlands, XLAB Slovenia

Dates
2013-02-01 to 2015-07-31
Participants Number
28
Website
http://www.botfree.eu; http://www.acdc-project.eu
Classification in CORDIS
Trustworthy Network Infrastructures, Mobile Devices and Smartphones, Technology&Tools,
Call
8
Budget
€ 15.500.000

HAVE A LOOK AT
As ACDC proceeds to become a European cyber defense center, it has opened it membership to external organizations. You can discover more information about membership and apply for it at: http://www.acdc-project.eu/?page_id=35

A toolbox to support high quality cryptographic software design

CACE

Computer Aided Cryptography Engineering

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)

Dates
2008-01-01 to 2010-12-31
Participants Number
12
Classification in CORDIS
Collaborative project
Call
1
Budget
€ 4.733.078

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

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.

A reliable data-centric information sharing

CONSEQUENCE

Context Aware Data-centric Information Sharing

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 f 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.

PILOT

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 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.

Coordinator
Europaeisches 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)

Dates
2008-01-01 to 2010-12-31
Participants Number
7
Website
http://www.consequence-project.eu/
Classification in CORDIS
Collaborative project
Call
1
Budget
€ 4.583.509