Advanced Software Protection:
Integration, Research and Exploitation

D7.02

ASPIRE Dissemination Plan

Project no.:	609734
Funding scheme:	Collaborative project
Start date of the project:	1st November 2013
Duration:	36 months
Work programme topic:	FP7-ICT-2013-10
Deliverable type:	Report
Deliverable reference number:	ICT-609734 / D7.02 / 1.01
WP and tasks contributing:	WP 7 / Tasks 7.1
Due date:	October 2014, M12
Actual submission date:	21 November 2014
Responsible Organization:	UGent
Editor:	Bjorn De Sutter
Dissemination Level:	Public
Revision:	1.01

Abstract:

We present an overview of the dissemination activities undertaken in year 1 of the project. We present an update to the global dissemination strategy as described in the Description of Work, and present individual dissemination plans of all project partners.

Keywords:
website, presentations, poster, leaflet, logo, workshops, publications, tutorials, press release

Editor

Bjorn De Sutter (UGent)

Contributors (ordered according to beneficiary numbers)

Cataldo Basile (POLITO)

Brecht Wyseur (NAGRA)

Mariano Ceccato (FBK)

Paolo Falcarin (UEL

Michael Zunke (SFNT)

Jerome D'Annovile (GTO)

The ASPIRE Consortium consists of:

Ghent University (UGent)	Coordinator & Beneficiary	Belgium
Politecnico Di Torino (POLITO)	Beneficiary	Italy
Nagravision SA (NAGRA)	Beneficiary	Switzerland
Fondazione Bruno Kessler (FBK)	Beneficiary	Italy
University of East London (UEL)	Beneficiary	UK
SFNT Germany GmbH (SFNT)	Beneficiary	Germany
Gemalto SA (GTO)	Beneficiary	France

Coordinating person:	Prof. Bjorn De Sutter
E-mail:	coordinator@aspire-fp7.eu
Tel:	+32 9 264 3367
Fax:	+32 9 264 3594
Project website:	www.aspire-fp7.eu

Disclaimer

The research leading to these results has received funding from the European Union Seventh Framework Programme (FP7/2007-2013) under grant agreement n° 609734.

The information in this document is provided as is and no guarantee or warranty is given that the information is fit for any particular purpose. The user thereof uses the information at its sole risk and liability.

Document Revision History

Version 1.0 21 Nov 2014	Original deliverable submitted to the EC.
Version 1.01 4 Dec 2014	Publication nr 7 by Mariano Ceccato (which was forgotten in v1.0) was added in Section 2.1. No other changes.

Executive Summary

This report first lists and details the dissemination activities undertaken by the consortium partners in Year 1 of the project. These activities can be summarized as follows:

- 6 scientific publications;
- a PowerPoint presentation template;
- 16 presentation activities where ASPIRE results were disseminated to expert audiences;
- 5 more such activities planned for early in Year 2;
- an accepted proposal for organizing the first ASPIRE workshop collocated with the International Conference on Software Engineering (ICSE) in May 2015;
- the ASPIRE project website, consisting of a public and private part;
- 10 dissemination activities to the general public, including press releases taken up by ACM TechNews, and an interview with the coordinator broadcasted on Flemish local public television at the time of the project kick-off meeting
- a project logo;
- a 4-page A4 project leaflet;
- an A0 project poster;
- social media activities (LinkedIn and Twitter);
- cooperation with other projects;
- the interview for the EU Yearbook compiled in the FP7 project SecCord.

Next, the deliverable presents the major project-wide dissemination plans for years two and three, as extensions and implementations of the project dissemination strategy that was already detailed in the project Description of Work, and that is partitioned into three phases: an awareness phase, a result phase, and an exploitation phase.

The main update to this strategy is that we plan to organize two workshops and one or more tutorials, collocated with major dissemination and networking events of different scientific communities, such as software engineering (see ICSE above), compiler technology (conference of the HiPEAC Network of Excellence), and software and system security.

Finally, each of the partners presents his individual plans for disseminating their results in years 2 and 3 of the project and following the project.

Contents

List of Figures

Section 1 Dissemination Strategy

Section Authors:

Bjorn De Sutter (UGent)

1.1 Initial Overall Dissemination Strategy

The initial ASPIRE dissemination strategy was first described in the DoW - Annex 1 Section B3.2.1 as follows:

Dissemination activities ensure the visibility and awareness of the project and support of the widest adoption of its results in industry and research. The external dissemination activities will be coordinated in WP7, in three phases.

Awareness phase

Raising public awareness involves the setting up of the basic marketing materials and awareness-raising presentations about the project and its goals. Thus, the main activities will be the following:

- *Setting up a common project design, such as an ASPIRE logo, templates for documents and presentations.*
- *Creating and maintaining the project website, which will describe the challenges and the goals of the project and which will introduce the project members.*
- *Designing the project information materials (such as a leaflet and an introductory off the shelf presentation), which can be distributed later on without investing greater efforts.*
- *Giving introductory presentations at conferences and workshops about the challenges and goals of ASPIRE to raise awareness among the scientific and industrial stakeholders and to establish the brand name of ASPIRE.*

Result phase

For promoting the results of the ASPIRE project, this phase will address stakeholders in software protection technology. The planned activities, mainly for but not limited to the non-industrial partners, are:

- *Display and promote public deliverables and news for viewing and downloading on the project website in order to show the liveliness and progress of the project and to keep interested parties up-to-date.*
- *Presentations at international conferences and workshops introducing the findings of the ASPIRE project. These presentations will still be research-oriented.*
- *The project will participate to the International Summer School on Information Security and Protection - Software Protection (ISSISP) when it comes back to Europe (scheduled for 2014) to disseminate results directly to PhD students and young researchers, but also to industrial participants.*
- *High-quality papers will be submitted to scientific and industry conferences.*
- *The ASPIRE consortium will publish and disseminate press releases after reaching important milestones.*

Currently, software protection is more art than an engineering discipline. In fact, in order to elaborate complicated tricks to protect the code, security experts need to spent at least the same amount of time as the potential attackers determined to port attacks. The ASPIRE project intends to promote the culture of an engineering approach to quantitative software *protection. The channels for the dissemination of the projects results therefore also include venues in the area of software engineering, measurements and empirical studies. In the area of software security, the main conferences and journals that ASPIRE will target include the ACM Conf. on Computer and Communications Security (CCS), Usenix Security Symp., IEEE Security & Privacy, IFIP Conf. on Communications and Multimedia Security, Symp. on Engineering Secure Software and Systems, and Whiley Journal of Security and Communication Networks. In the area of software engineering, measurements and empirical studies, ASPIRE will consider ACM Trans. on Software Engineering and Methodology, IEEE Trans. on Software Engineering, ACM Conf. on Software Engineering, IEEE Working Conf. on Source Code Analysis and Manipulation, IEEE Conf. on Program Comprehension, IEEE Working Conf. on Reverse Engineering, Symposium on Empirical Software Engineering and Measurement (ESEM) and Workshop on Measurability of Security in Software Architectures, among others.*

Exploitation phase

Specific activities of this phase, mainly for but not limited to, the industrial partners include:

- *Exploitation-oriented upgrade of the project website, including optimisation for search engines and optional registration for specific keywords.*
- *Participation at several exhibitions, fairs and workshops, where the results of the project could be presented to business stakeholders and contacts for potential commercial projects could be built.*
- *Organization of an ASPIRE workshop collocated with a major networking event or conference.*
- *Individualised demonstrations for interested stakeholders during the negotiation of business projects.*

The result and exploitation-oriented dissemination activities will be planned in M12 of the project in the form of a Dissemination Plan deliverable (D6.02). At the end of the project, a Dissemination Report will be delivered (D7.04). Detailed descriptions of the individual partners' dissemination strategies are presented in Annex II.

1.2 Status after Year 1

All activities of the awareness phase have been conducted as originally planned. Also the activities for the Result phase and the Exploitation phase as documented later in this deliverable are a direct realization of the above strategy.

Section 2 Dissemination Activities Started in M01-M12

Section Authors:

Bjorn De Sutter (UGent)

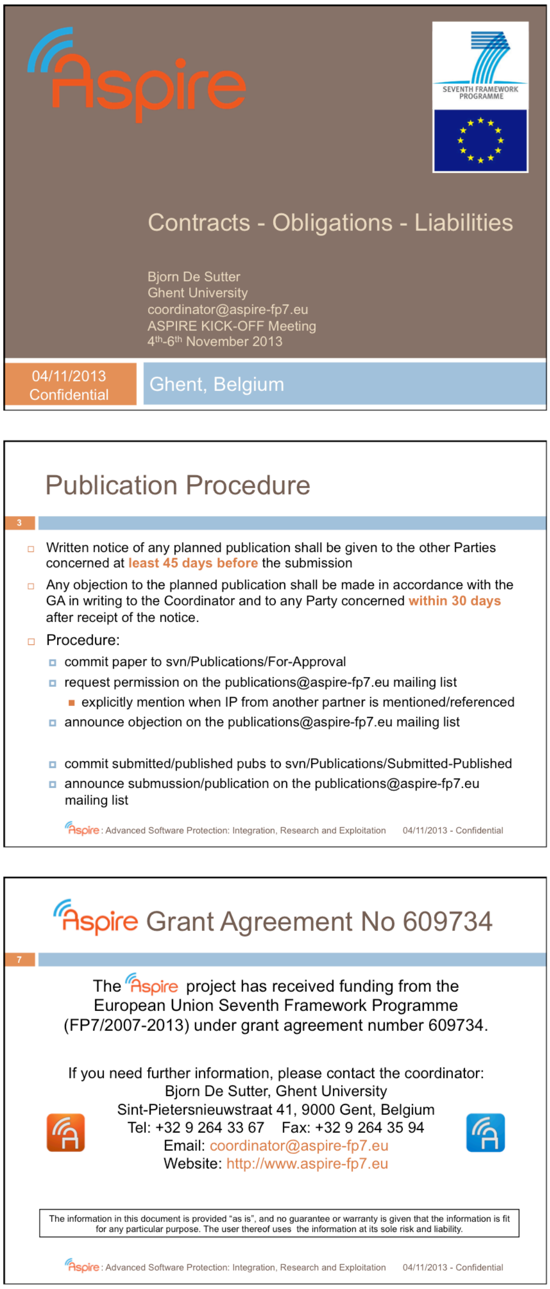
2.1 Scientific Publications

1. Yosief Weldezghi Frezghi
   Code Diversity: Code Obfuscation and Clustering Heuristic to Prevent Code Tampering
   Master Thesis, University of Trento, Department of Information Engineering and Computer Science. Advisor: Luigi Palopoli, Second Supervisor: Mariano Ceccato. Academic Year 2013-2014
2. Biniam Fisseha Demissie
   Implementation and Assessment of Data Obfuscation for C/C++ Code Based on Residue Number Coding.
   Master Thesis, University of Trento, Department of Information Engineering and Computer Science. Advisor: Bruno Crispo, Second Supervisors: Mariano Ceccato and Roberto Tiella. Academic Year 2013-2014.
3. Bjorn De Sutter
   Evaluating the Strength of Software Protections (Abstract)
   Challenges in Analysing Executables: Scalability, Self-Modifying Code and Synergy, Report from Dagstuhl Seminar 14241, 2014, p. 54
4. Paolo Tonella, Mariano Ceccato, Bjorn De Sutter, Bart Coppens
   A Measurement Framework to Quantify Software Protections (Poster + Extended Abstract)
   Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, 2014, p. 1505-1507.
5. Bjorn De Sutter
   Towards a Unified Framework for Evaluating the Strength of Software Protections
   (Extended Abstract)
   Proc. of the ARO Workshop on Continuously Upgradeable Software Security and Protection, 2014, p. 34-35.
6. Brecht Wyseur
   Reflections on Software Renewability from an Industry Perspective (Extended Abstract)
   Proc. of the ARO Workshop on Continuously Upgradeable Software Security and Protection, 2014, p. 36-37.
7. Mariano Ceccato
   On the Need for More Human Studies to Assess Software Protection (Extended Abstract)
   Proc. of the ARO Workshop on Continuously Upgradeable Software Security and Protection, 2014, p. 55-56.

2.2 Presentations, Participation in Conferences

2.2.1 Presentation Template

In order to streamline the dissemination of ASPIRE results and create a recognition of ASPIRE graphical material in the software protection community, a PowerPoint presentation template was designed. Some example slides are depicted in Figure 1.



Contracts - Obligations - Liabilities

Bjorn De Sutter
Ghent University
coordinator@aspire-fp7.eu
ASPIRE KICK-OFF Meeting
4th-6th November 2013

04/11/2013
Confidential

Ghent, Belgium

Publication Procedure

3

- Written notice of any planned publication shall be given to the other Parties concerned at **least 45 days before** the submission
- Any objection to the planned publication shall be made in accordance with the GA in writing to the Coordinator and to any Party concerned **within 30 days** after receipt of the notice.
- Procedure:
  - commit paper to svn/Publications/For-Approval
  - request permission on the publications@aspire-fp7.eu mailing list
    - explicitly mention when IP from another partner is mentioned/referenced
  - announce objection on the publications@aspire-fp7.eu mailing list
  - commit submitted/published pubs to svn/Publications/Submitted-Published
  - announce submussion/publication on the publications@aspire-fp7.eu mailing list

Aspire: Advanced Software Protection: Integration, Research and Exploitation 04/11/2013 - Confidential

Aspire Grant Agreement No 609734

7

The Aspire project has received funding from the European Union Seventh Framework Programme (FP7/2007-2013) under grant agreement number 609734.

If you need further information, please contact the coordinator:
Bjorn De Sutter, Ghent University
Sint-Pietersnieuwstraat 41, 9000 Gent, Belgium
Tel: +32 9 264 33 67 Fax: +32 9 264 35 94
Email: coordinator@aspire-fp7.eu
Website: http://www.aspire-fp7.eu

The information in this document is provided "as is", and no guarantee or warranty is given that the information is fit for any particular purpose. The user thereof uses the information at its sole risk and liability.

Aspire: Advanced Software Protection: Integration, Research and Exploitation 04/11/2013 - Confidential

Figure 1 - Examples of ASPIRE presentation template

2.2.2 Activities in M01-M12

1.	Activity:	Conference
	Main Leader:	Bjorn De Sutter, UGent
	Title:	A Golden Standard for Evaluating Software Protection against Man-at-the-End Attacks
	Place:	Vienna (AU)
	Date:	20/01/2014
	Audience Size:	25
	Type and Goal Event:	Keynote speech at the Cryptography and Security in Computing Systems (CS^2) workshop (col. with the HiPEAC conference)
	Countries Addresses:	International
	URL:	https://aspire-fp7.eu/content/about

2. Activity: Exhibition
   Main Leader: Brecht Wyseur, NAGRA
   Title: ASPIRE: Advanced Software Protection: Integration, Research and Exploitation
   Place: Brussels (BE)
   Date: 28/03/2014
   Audience Size: 480
   Type and Goal Event: Poster at the EU Cybersecurity Strategy - High Level Conference
   Countries Addresses: International

3. Activity: Presentation
   Main Leader: Paolo Falcarin, UEL
   Title: Software Protection Research Overview
   Place: London (UK)
   Date: 20/01/2014
   Audience Size: 20
   Type and Goal Event: Internal presentation to research development team at UEL to plan for knowledge transfer and collaborations
   Countries Addresses: National

4. Activity: Presentation
   Main Leader: Cataldo Basile, POLITO
   Title: ASPIRE: Advanced Software Protection: Integration, Research and Exploitation
   Place: Torino (Italy)
   Date: 26/02/2014
   Audience Size: 15
   Type and Goal Event: Internal presentation to the TORSEC group of Politecnico di Torino
   Countries Addresses: National

5. Activity: Presentation
   Main Leader: Cataldo Basile, POLITO
   Title: ASPIRE: Advanced Software Protection: Integration, Research and Exploitation
   Place: Torino (Italy)
   Date: 14/03/2014
   Audience Size: 20
   Type and Goal Event: Internal presentation to SECURED team of the Politecnico di Torino
   Countries Addresses: National

6. Activity: Presentation
   Main Leader: Antonio Lioy, POLITO
   Title: ASPIRE: Advanced Software Protection: Integration, Research and Exploitation
   Place: Torino (Italy)
   Date: 5/12/2013
   Audience Size: 150
   Type and Goal Event: Presentation of the ASPIRE project to the Master students of the course 03GSD “Sicurezza dei sistemi informatici” (Computer systems security)
   Countries Addresses: National

7. Activity: Presentation
   Main Leader: Antonio Lioy, POLITO
   Title: ASPIRE: Advanced Software Protection: Integration, Research and Exploitation
   Place: Torino (Italy)
   Date: 9/12/2013
   Audience Size: 100
   Type and Goal Event: Presentation of the ASPIRE project to the Master students of the course 02KRQ “Computer System Security”
   Countries Addresses: National

8. Activity: Presentation
   Main Leader: Paolo Falcarin, UEL
   Title: Software Protection
   Place: London (UK)
   Date: 30/04/2014
   Audience Size: 20
   Type and Goal Event: UEL Expert Series: academics are invited to present their work to audience of small-medium enterprises
   Countries Addresses: National

9. Activity: Presentation
   Main Leader: Mariano Ceccato, FBK
   Title: Code Diversity: Code Obfuscation and Clustering Heuristic to Prevent Code Tampering
   Place: Trento (IT)
   Date: 12/03/2014
   Audience Size: 30
   Type and Goal Event: Master thesis defense by Yosief Weldezghi Frezghi, under supervision of Mariano Ceccato
   Countries Addresses: National

10. Activity: Presentation
    Main Leader: Bjorn De Sutter, UGent
    Title: Evaluating the strength of software protections
    Place: Dagstuhl (DE)
    Date: 11/06/2014
    Audience Size: 44
    Type and Goal Event: Dagstuhl Seminar on "Challenges in Analysing Executables: Scalability, Self-Modifying Code and Synergy"
    Countries Addresses: International
    URL: http://www.dagstuhl.de/en/program/calendar/semhp/?semnr=14241

11. Activity: Lecture
    Main Leader: Bjorn De Sutter, UGent
    Title: Evaluating the strength of software protections
    Place: Verona (IT)
    Date: 30/07/2014
    Audience Size: 35
    Type and Goal Event: Lecture of 3 hours at ISSISP Summer School on Software Protection,
    Countries Addresses: International
    URL: http://issisp2014.di.univr.it/

12. Activity: Lecture
    Main Leader: Brecht Wyseur, NAGRA
    Title: White-box Cryptography
    Place: Verona (IT)
    Date: 28/07/2014
    Audience Size: 35
    Type and Goal Event: Lecture of 3 hours at ISSISP Summer School on Software Protection,
    Countries Addresses: International
    URL: http://issisp2014.di.univr.it/

13. Activity: Presentation
    Main Leader: Jens Van den Broeck, UGent
    Title: The ASPIRE project
    Place: Verona (IT)
    Date: 31/07/2014
    Audience Size: 35
    Type and Goal Event: Poster presentation at ISSISP Summer School on Software Protection,
    Countries Addresses: International
    URL: http://issisp2014.di.univr.it/

14. Activity: Presentation
    Main Leader: Brecht Wyseur, NAGRA
    Title: An introduction to ASPIRE
    Place: Cheseaux, CH
    Date: 10/09/2014
    Audience Size: 50
    Type and Goal Event: Brecht presented the project to NAGRA's group-wide security experts

15. Activity: Presentation
    Main Leader: Brecht Wyseur, NAGRA
    Title: The ASPIRE use case demonstrator
    Place: Cheseaux, CH
    Date: 11/09/2014
    Audience Size: 20
    Type and Goal Event: Presentation during company internal Technical Session Workshop

16. Activity: Presentation
    Main Leader: Mariano Ceccato, FBK
    Title: Implementation and Assessment of Data Obfuscation for C/C++ Code Based on Residue Number Coding
    Place: Trento (IT)
    Date: 14/10/2014
    Audience Size: 30
    Type and Goal Event: Master thesis defense by Biniam Fisseha Demissie, under supervision of Mariano Ceccato
    Countries Addresses: National

2.2.3 Upcoming ASPIRE Dissemination Activities

1. Activity: Conference
   Main Leader: Mariano Ceccato, FBK
   Title: A Measurement Framework to Quantify Software Protections
   Place: Scottsdale (USA)
   Date: 04/11/2014
   Audience Size: 400-500
   Type and Goal Event: Poster presentation at 21st ACM Conference on Computer and Communications Security (AACM CCS 2014)
   Countries Addresses: International
   URL: http://www.sigsac.org/ccs/CCS2014/pro_poster.html
   Note: Due to sickness of the presenter, this presentation was cancelled at the last minute

2. Activity: Conference
   Main Leader: Bjorn De Sutter, UGent
   Title: Towards a Unified Framework for Evaluating the Strength of Software Protection
   Place: Scottsdale (USA)
   Date: 07/11/2014
   Audience Size: 25
   Type and Goal Event: Invited position paper, ARO Workshop on Continuously Upgradeable Software Security and Protection
   Countries Addresses: International
   URL: http://ssp2014.di.univr.it/

3. Activity: Conference
   Main Leader: Brecht Wyseur, NAGRA
   Title: Reflections on Software Renewability from an Industry Perspective
   Place: Scottsdale (USA)
   Date: 07/11/2014
   Audience Size: 25
   Type and Goal Event: Invited position paper, ARO Workshop on Continuously Upgradeable Software Security and Protection

	Countries Addresses:	International
	URL:	http://ssp2014.di.univr.it/
4.	Activity:	Conference
	Main Leader:	Bjorn De Sutter, UGent
	Title:	The ASPIRE project
	Place:	Amsterdam (NL)
	Date:	21/01/2015
	Audience Size:	500
	Type and Goal Event:	Poster presentation at the HiPEAC Conference 2015
	Countries Addresses:	International
5.	Activity:	Conference
	Main Leader:	Bjorn De Sutter, UGent
	Title:	The ASPIRE project
	Place:	Amsterdam (NL)
	Date:	20/01/2015
	Audience Size:	-
	Type and Goal Event:	Poster presentation at the 3rd Workshop on Transfer to Industry and Start-Ups
	Countries Addresses:	International

2.2.4 First ASPIRE workshop

In its description of Task T7.1, the ASPIRE DoW has foreseen the organization of an ASPIRE workshop to serve as a dissemination and networking event.

In the project dissemination plan, we propose to go further than one workshop, and to organize multiple workshops, collocated with conferences that attract researchers and practitioners in different related fields. For the first such workshop, we target the he 37th International Conference on Software Engineering (ICSE, http://2015.icse-conferences.org/) that will be organized in Florence (IT) on 16-24 May 2015. With such a workshop, we aim to reach the software-engineering community, with which we want to interact regarding the usability aspects of ASPIRE technology in the hands of non-security experts.

On 10 October, a workshop proposal was submitted to ICSE. It is included in Appendix A.

On 20 November, we got the notification from the ICSE Workshop Committee Co-Chairs that the proposal was accepted. We will hence commence its organization and the design of a workshop website shortly.

2.3 ASPIRE Project Website

2.3.1 Public ASPIRE Website http://www.aspire-fp7.eu

To serve the broadest possible visibility of the project, the project website was launched in the first month of the project. The website builds on the Drupal Content Management System (https://drupal.org/). All pages on this public website are available for everyone, it is not necessary to login.

The website can be accessed with all major browsers, and a Drupal Theme was licensed and is used that automatically adapts and reformats the page layout for the screen sizes and resolutions used on today's wide variety of Internet access points, ranging from small, touchscreen smart phones, over larger screen tablets, to laptops and desktop computers.

The website will be maintained until three years after the end of the project.

After its initial launch, content has been gradually added to the website to turn it into a kind of software protection knowledge base.

Currently, the public part of the website consists of the following pages:

- **Home**: General introduction to the project, brief overview of consortium by means of partner logos. See Figure 2 and Figure 3 for screenshots of the p home age on a desktop browser. Figure 4 shows a screenshot on the iOS smartphone browser as demonstration of the portability of the used theme.
- **Consortium**: Description of all project partners and their principal investigators. See Figure 5.
- **Contact**: Contact form and coordinator contact information.
- **About**: Some more information about the project, and links to press releases and presentations about the project by the coordinator. See Figure 6.
- **Knowledge Base**: A publication database can be interfaced through the ASPIRE website knowledge base. Currently the publications can be selected and ranked based on subject (metrics, obfuscations, program analyses, ...) and year. See Figure 7.
- **Related**: A page where links to related journals, conferences, summer schools, projects, etc. will be maintained. See Figure 8.
- **Deliverables**: A webpage that lists all project deliverables, where public ones will be made available once accepted by the EC. See Figure 9.

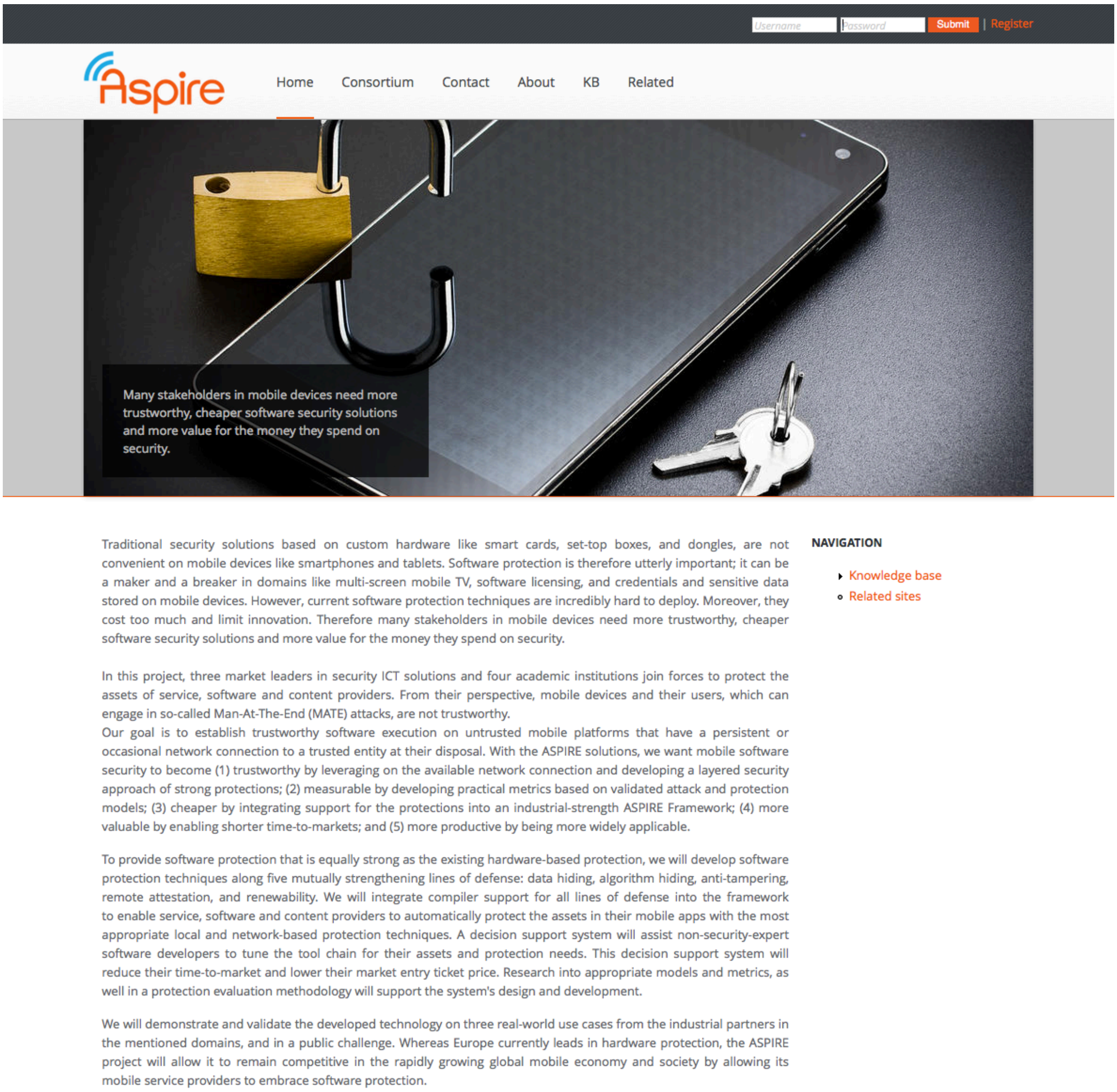
Early on in year two, when the project enters the results phase in which the first major publishable results and milestones should be achieved, a news page will be added that will continuously be updated with relevant project news and related news.

From year two on, when the ASPIRE Compiler Tool Chain can be deployed on more than toy examples and when more protections can be applied, the project coordinator and the responsible for dissemination will also create short demonstration videos to be placed online, e.g., on YouTube or Vimeo, and linked on the website.

Due to a configuration issue that was not resolved until late May 2014, we can only present Google Analytics results for the period June 2014 - now:

month	sessions	users	new users
June	169	105	57.40%
July	160	124	68.12%
August	157	128	74.52%
September	262	179	61.83%
October	226	160	61.50%

As shown in Figure 10, which depicts the number of new users per country, the ASPIRE website draws worldwide attention.



Many stakeholders in mobile devices need more trustworthy, cheaper software security solutions and more value for the money they spend on security.

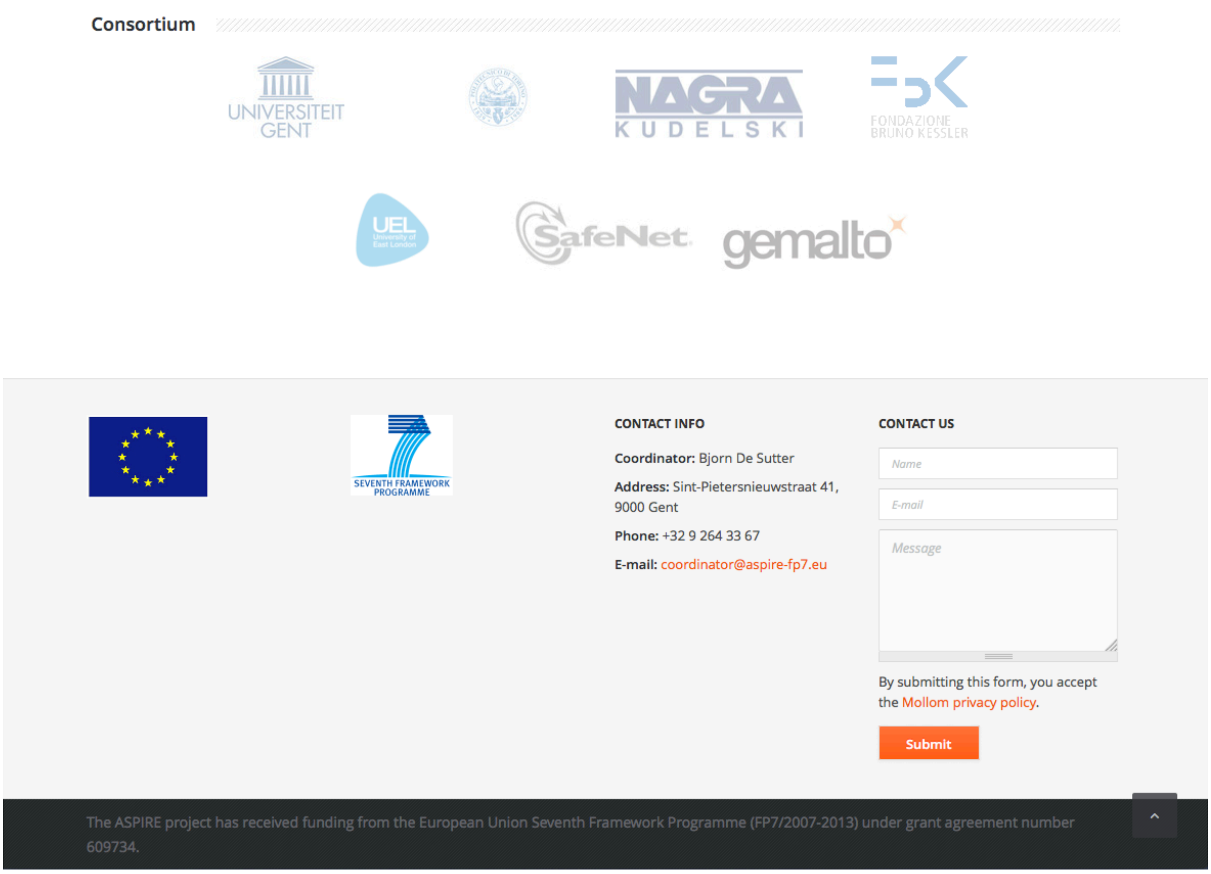
Traditional security solutions based on custom hardware like smart cards, set-top boxes, and dongles, are not convenient on mobile devices like smartphones and tablets. Software protection is therefore utterly important; it can be a maker and a breaker in domains like multi-screen mobile TV, software licensing, and credentials and sensitive data stored on mobile devices. However, current software protection techniques are incredibly hard to deploy. Moreover, they cost too much and limit innovation. Therefore many stakeholders in mobile devices need more trustworthy, cheaper software security solutions and more value for the money they spend on security.

In this project, three market leaders in security ICT solutions and four academic institutions join forces to protect the assets of service, software and content providers. From their perspective, mobile devices and their users, which can engage in so-called Man-At-The-End (MATE) attacks, are not trustworthy.
Our goal is to establish trustworthy software execution on untrusted mobile platforms that have a persistent or occasional network connection to a trusted entity at their disposal. With the ASPIRE solutions, we want mobile software security to become (1) trustworthy by leveraging on the available network connection and developing a layered security approach of strong protections; (2) measurable by developing practical metrics based on validated attack and protection models; (3) cheaper by integrating support for the protections into an industrial-strength ASPIRE Framework; (4) more valuable by enabling shorter time-to-markets; and (5) more productive by being more widely applicable.

To provide software protection that is equally strong as the existing hardware-based protection, we will develop software protection techniques along five mutually strengthening lines of defense: data hiding, algorithm hiding, anti-tampering, remote attestation, and renewability. We will integrate compiler support for all lines of defense into the framework to enable service, software and content providers to automatically protect the assets in their mobile apps with the most appropriate local and network-based protection techniques. A decision support system will assist non-security-expert software developers to tune the tool chain for their assets and protection needs. This decision support system will reduce their time-to-market and lower their market entry ticket price. Research into appropriate models and metrics, as well in a protection evaluation methodology will support the system's design and development.

We will demonstrate and validate the developed technology on three real-world use cases from the industrial partners in the mentioned domains, and in a public challenge. Whereas Europe currently leads in hardware protection, the ASPIRE project will allow it to remain competitive in the rapidly growing global mobile economy and society by allowing its mobile service providers to embrace software protection.

Figure 2 - Screenshot of the top part of the home page on the ASPIRE website



CONTACT INFO

Coordinator: Bjorn De Sutter

Address: Sint-Pietersnieuwstraat 41, 9000 Gent

Phone: +32 9 264 33 67

E-mail: coordinator@aspire-fp7.eu

CONTACT US

Name

E-mail

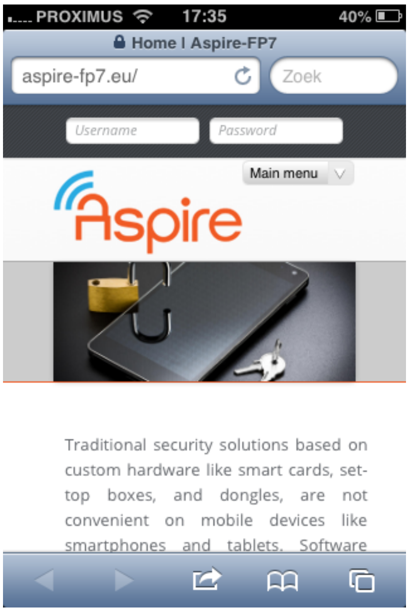
Message

By submitting this form, you accept the Mollom privacy policy.

Submit

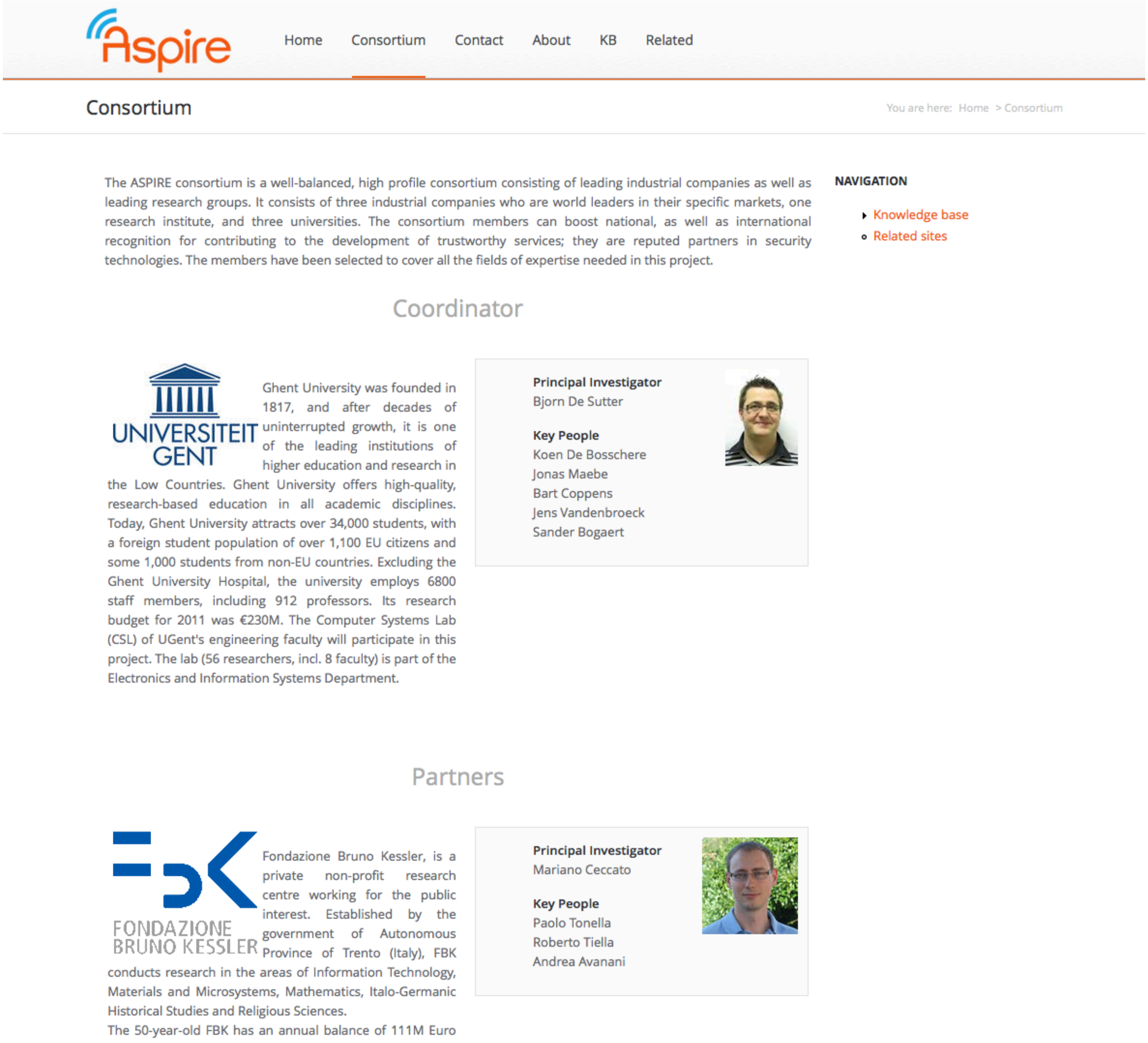
The ASPIRE project has received funding from the European Union Seventh Framework Programme (FP7/2007-2013) under grant agreement number 609734.

Figure 3 - Screenshot of the bottom part of the home page on the ASPIRE website



Traditional security solutions based on custom hardware like smart cards, set-top boxes, and dongles, are not convenient on mobile devices like smartphones and tablets. Software

Figure 4 - Screenshot of the ASPIRE website home page on an (old) iPhone 3G.



Consortium

The ASPIRE consortium is a well-balanced, high profile consortium consisting of leading industrial companies as well as leading research groups. It consists of three industrial companies who are world leaders in their specific markets, one research institute, and three universities. The consortium members can boost national, as well as international recognition for contributing to the development of trustworthy services; they are reputed partners in security technologies. The members have been selected to cover all the fields of expertise needed in this project.

NAVIGATION

- Knowledge base
- Related sites

Coordinator

UNIVERSITEIT GENT

Ghent University was founded in 1817, and after decades of uninterrupted growth, it is one of the leading institutions of higher education and research in the Low Countries. Ghent University offers high-quality, research-based education in all academic disciplines. Today, Ghent University attracts over 34,000 students, with a foreign student population of over 1,100 EU citizens and some 1,000 students from non-EU countries. Excluding the Ghent University Hospital, the university employs 6800 staff members, including 912 professors. Its research budget for 2011 was €230M. The Computer Systems Lab (CSL) of UGent's engineering faculty will participate in this project. The lab (56 researchers, incl. 8 faculty) is part of the Electronics and Information Systems Department.

Principal Investigator
Bjorn De Sutter

Key People
Koen De Bosschere
Jonas Maebe
Bart Coppens
Jens Vandenbroeck
Sander Bogaert

Partners

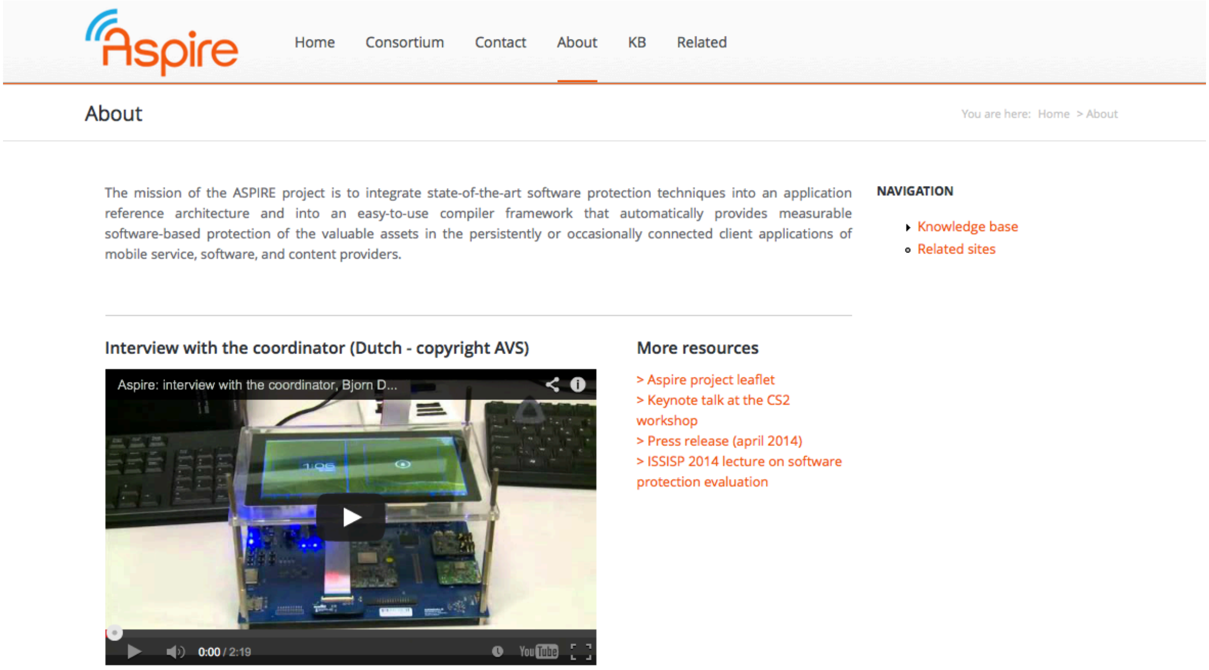
FONDAZIONE BRUNO KESSLER

Fondazione Bruno Kessler, is a private non-profit research centre working for the public interest. Established by the government of Autonomous Province of Trento (Italy), FBK conducts research in the areas of Information Technology, Materials and Microsystems, Mathematics, Italo-Germanic Historical Studies and Religious Sciences.
The 50-year-old FBK has an annual balance of 111M Euro

Principal Investigator
Mariano Ceccato

Key People
Paolo Tonella
Roberto Tiella
Andrea Avanani

Figure 5 - Screenshot of the consortium page on the ASPIRE website


Aspire
Home
Consortium
Contact
About
KB
Related
You are here: Home > About
Aspire: interview with the coordinator, Bjorn D...
0:00 / 2:19
YouTube

About

The mission of the ASPIRE project is to integrate state-of-the-art software protection techniques into an application reference architecture and into an easy-to-use compiler framework that automatically provides measurable software-based protection of the valuable assets in the persistently or occasionally connected client applications of mobile service, software, and content providers.

Interview with the coordinator (Dutch - copyright AVS)

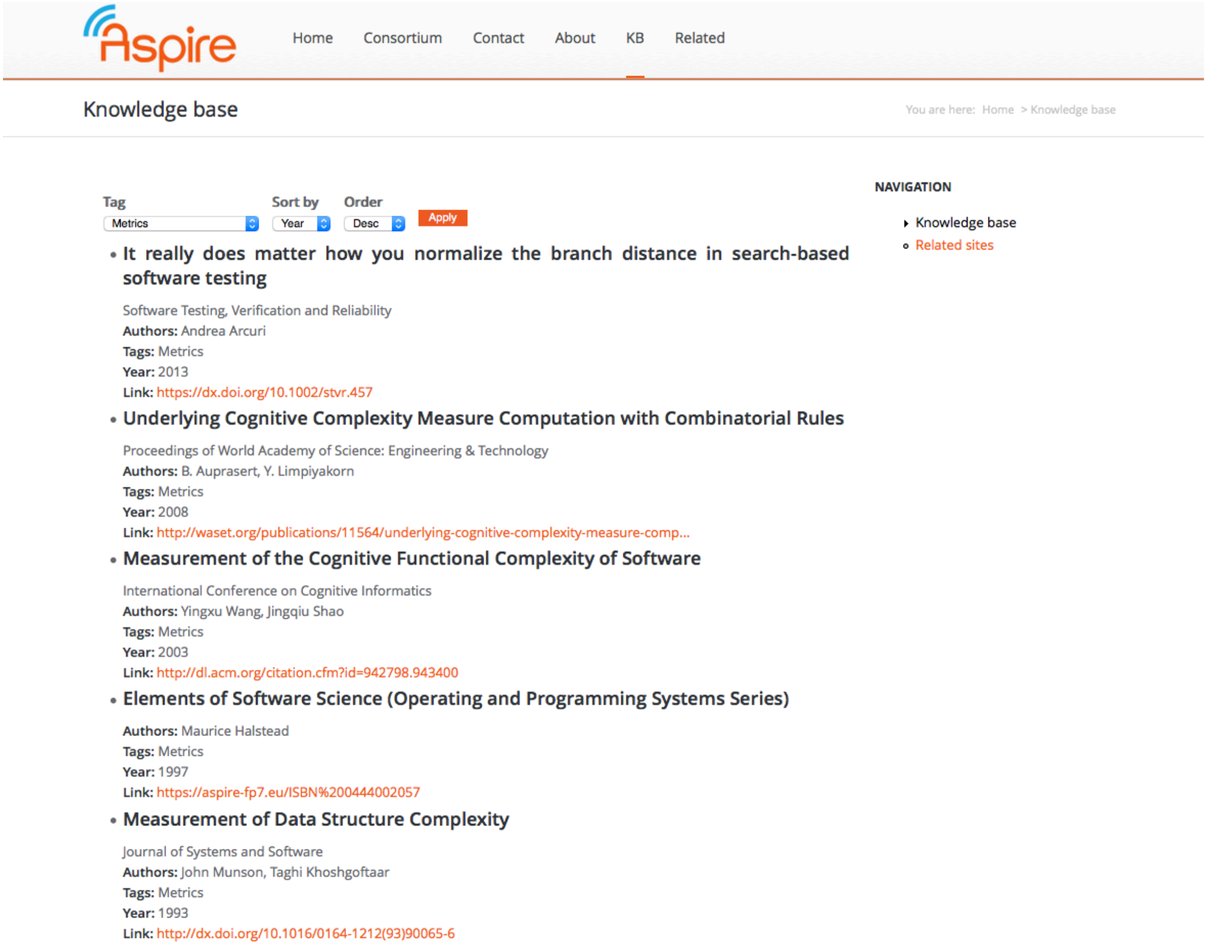
More resources

> Aspire project leaflet
> Keynote talk at the CS2 workshop
> Press release (april 2014)
> ISSISP 2014 lecture on software protection evaluation

NAVIGATION

- Knowledge base
- Related sites

Figure 6 - Screenshot of the about page with links to presentations on the ASPIRE website



Knowledge base

Tag: Metrics Sort by: Year Order: Desc

- **It really does matter how you normalize the branch distance in search-based software testing**

  Software Testing, Verification and Reliability
  Authors: Andrea Arcuri
  Tags: Metrics
  Year: 2013
  Link: https://dx.doi.org/10.1002/stvr.457

- **Underlying Cognitive Complexity Measure Computation with Combinatorial Rules**

  Proceedings of World Academy of Science: Engineering & Technology
  Authors: B. Auprasert, Y. Limpiyakorn
  Tags: Metrics
  Year: 2008
  Link: http://waset.org/publications/11564/underlying-cognitive-complexity-measure-comp...

- **Measurement of the Cognitive Functional Complexity of Software**

  International Conference on Cognitive Informatics
  Authors: Yingxu Wang, Jingqiu Shao
  Tags: Metrics
  Year: 2003
  Link: http://dl.acm.org/citation.cfm?id=942798.943400

- **Elements of Software Science (Operating and Programming Systems Series)**

  Authors: Maurice Halstead
  Tags: Metrics
  Year: 1997
  Link: https://aspire-fp7.eu/ISBN%200444002057

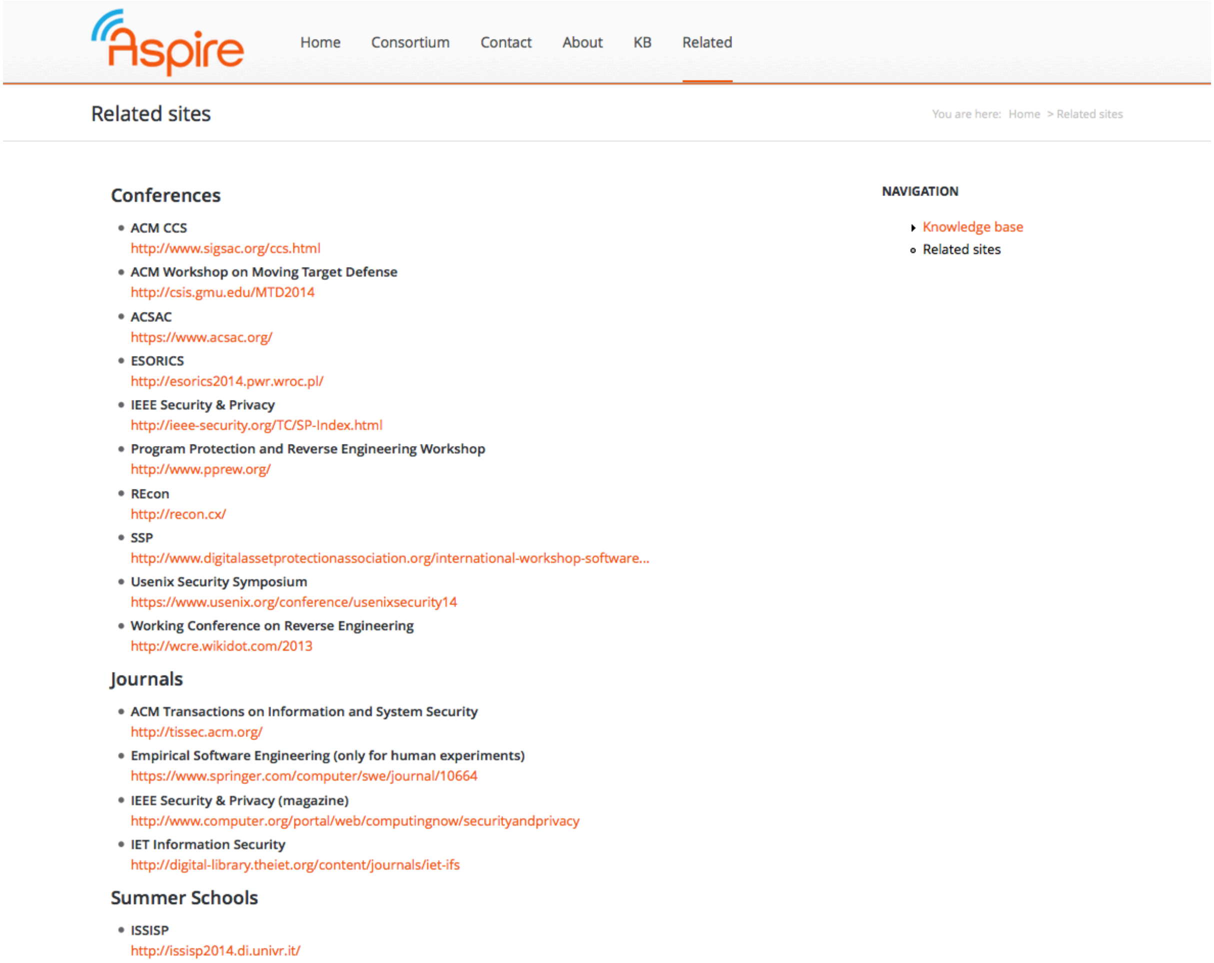
- **Measurement of Data Structure Complexity**

  Journal of Systems and Software
  Authors: John Munson, Taghi Khoshgoftaar
  Tags: Metrics
  Year: 1993
  Link: http://dx.doi.org/10.1016/0164-1212(93)90065-6

NAVIGATION

- Knowledge base
- Related sites

Figure 7 - Screenshot of the knowledge base page on the ASPIRE website



Related sites

Conferences

- ACM CCS
  http://www.sigsac.org/ccs.html
- ACM Workshop on Moving Target Defense
  http://csis.gmu.edu/MTD2014
- ACSAC
  https://www.acsac.org/
- ESORICS
  http://esorics2014.pwr.wroc.pl/
- IEEE Security & Privacy
  http://ieee-security.org/TC/SP-Index.html
- Program Protection and Reverse Engineering Workshop
  http://www.pprew.org/
- REcon
  http://recon.cx/
- SSP
  http://www.digitalassetprotectionassociation.org/international-workshop-software...
- Usenix Security Symposium
  https://www.usenix.org/conference/usenixsecurity14
- Working Conference on Reverse Engineering
  http://wcre.wikidot.com/2013

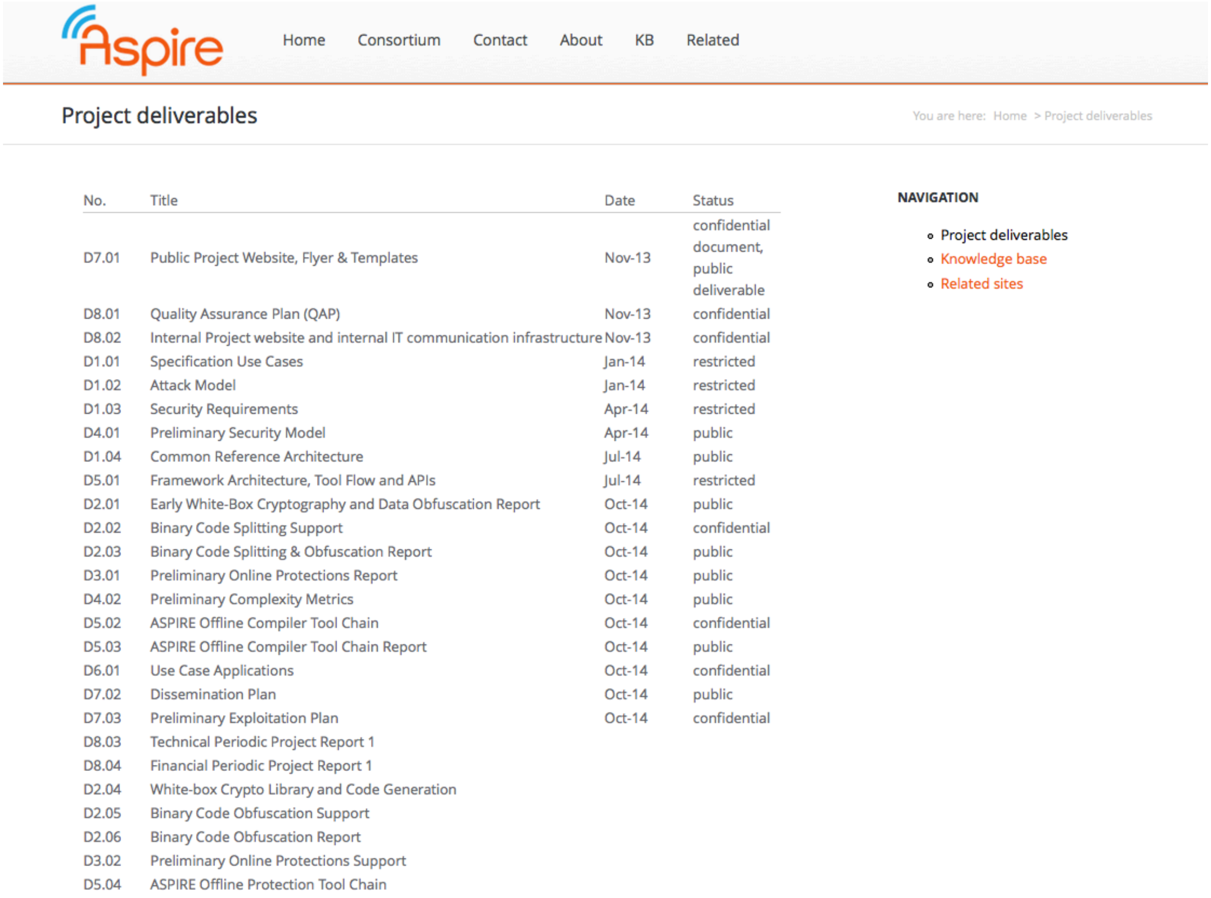
Journals

- ACM Transactions on Information and System Security
  http://tissec.acm.org/
- Empirical Software Engineering (only for human experiments)
  https://www.springer.com/computer/swe/journal/10664
- IEEE Security & Privacy (magazine)
  http://www.computer.org/portal/web/computingnow/securityandprivacy
- IET Information Security
  http://digital-library.theiet.org/content/journals/iet-ifs

Summer Schools

- ISSISP
  http://issisp2014.di.univr.it/

Figure 8 - Screenshot of the related work page on the ASPIRE website



Project deliverables

No.	Title	Date	Status
D7.01	Public Project Website, Flyer & Templates	Nov-13	confidential document, public deliverable
D8.01	Quality Assurance Plan (QAP)	Nov-13	confidential
D8.02	Internal Project website and internal IT communication infrastructure	Nov-13	confidential
D1.01	Specification Use Cases	Jan-14	restricted
D1.02	Attack Model	Jan-14	restricted
D1.03	Security Requirements	Apr-14	restricted
D4.01	Preliminary Security Model	Apr-14	public
D1.04	Common Reference Architecture	Jul-14	public
D5.01	Framework Architecture, Tool Flow and APIs	Jul-14	restricted
D2.01	Early White-Box Cryptography and Data Obfuscation Report	Oct-14	public
D2.02	Binary Code Splitting Support	Oct-14	confidential
D2.03	Binary Code Splitting & Obfuscation Report	Oct-14	public
D3.01	Preliminary Online Protections Report	Oct-14	public
D4.02	Preliminary Complexity Metrics	Oct-14	public
D5.02	ASPIRE Offline Compiler Tool Chain	Oct-14	confidential
D5.03	ASPIRE Offline Compiler Tool Chain Report	Oct-14	public
D6.01	Use Case Applications	Oct-14	confidential
D7.02	Dissemination Plan	Oct-14	public
D7.03	Preliminary Exploitation Plan	Oct-14	confidential
D8.03	Technical Periodic Project Report 1		
D8.04	Financial Periodic Project Report 1		
D2.04	White-box Crypto Library and Code Generation		
D2.05	Binary Code Obfuscation Support		
D2.06	Binary Code Obfuscation Report		
D3.02	Preliminary Online Protections Support		
D5.04	ASPIRE Offline Protection Tool Chain		

Figure 9 - Screenshot of the ASPIRE webpage with the list of deliverables

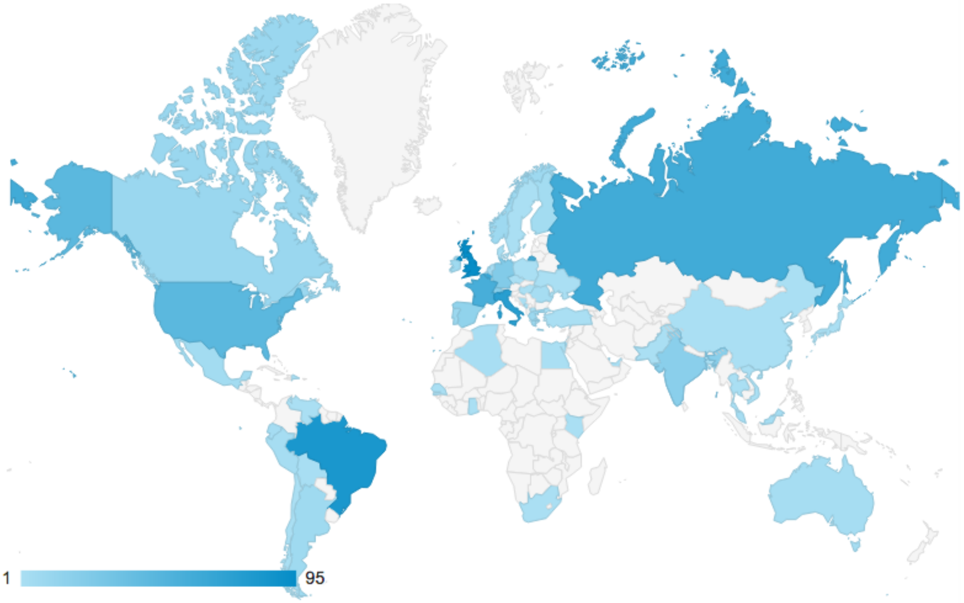


Figure 10 - Unique users per country visiting the ASPIRE website since June 2014

2.3.2 Restricted Area of ASPIRE Website

As can be seen at the top of the screenshot in Figure 2, the ASPIRE website allows consortium members to register and log in to the website. After doing so, the private part of the website can be accessed.

This part includes

- **wiki** pages used for internal dissemination of relevant information that needs to be updated regularly;
- a **Steering Board** page linking and listing all information regarding the boards' meetings, such as agendas and minutes;
- an **action tracker** page listing all ongoing actions, deadlines, progress states, etc.;
- **mailing list archives**;
- the project **SVN repository**.

2.4 Presentation of the Project to the General Public

2.4.1 Web, Press Releases, Articles in Popular Press, TV Footage

1.	Activity:	Web
	Main Leader:	UGent
	Title:	ASPIRE Public Website
	Date:	01/11/2013
	Audience Size:	-
	Type and Goal Event:	Website goes online
	Countries Addresses:	International
	URL:	https://www.aspire-fp7.eu/

2.	Activity:	Press Release
	Main Leader:	UGent
	Title:	Gentse onderzoekers ontwikkelen sterke bescherming voor mobiele software en diensten.
	Date:	04/11/2013
	Type and Goal Event:	Online press release
	Countries Addresses:	Belgium
	URL:	http://www.ugent.be/ea/nl/actueel/nieuws/gentse-onderzoekers-ontwikkelen-sterke-bescherming-voor-mobiele-software-en-diensten.htm

This press release is taken up on other news sites, including the Student Paper of Ghent University (http://www.schamper.ugent.be/2013-online/aspire-is-watching-you), Engineeringnet.be (http://engineeringnet.be/belgie/detail_belgie.asp?Id=11280&titel=Gentse%20onderzoekers%20zetten%20tanden%20in%20mobiele%20databescherming&category=nieuws), and the news page of the Faculty of Engineering and Architecture of UGent (http://www.ugent.be/ea/nl/actueel/nieuws/gentse-onderzoekers-ontwikkelen-sterke-bescherming-voor-mobiele-software-en-diensten.htm)

3.	Activity:	News Report on Television
	Main Leader:	Bjorn De Sutter, UGent
	Title:	AVS News - The ASPIRE Project
	Date:	05/11/2013
	Audience Size:	-
	Type and Goal Event:	The coordinator was interviewed, most of the interview was broadcasted on the local television station AVS in the province of Eastern Flanders in Belgium. The interview was mixed with information about the project, and footage taken during the project kick-off meeting. The whole report/news item lasted 2.18 minutes. A screenshot is shown in Figure 11.
	Countries Addresses:	Belgium

4.	Activity:	Web
	Main Leader:	UEL

Title: €460,000 to develop software protection
Date: 01/12/2013
Audience Size: -
Type and Goal Event: ASPIRE project is presented on UEL website
Countries Addresses: UK
URL: http://www.uel.ac.uk/research/news/aspire/

5. Activity: Web
Main Leader: GTO
Title: The ASPIRE F7 project
Date: 06/12/2013
Audience Size: Company
Type and Goal Event: Wiki page on the Gemalto Intranet describing the project and expected results

6. Activity: Web
Main Leader: NAGRA
Title: The ASPIRE F7 project
Date: 13/03/2014
Audience Size: Company, 3000+
Type and Goal Event: a post describing ASPIRE project has been published on Nagravision intranet's blog

7. Activity: Press Release
Main Leader: Bjorn De Sutter, UGent
Title: ASPIRE project to bring strong software protection to mobile devices
Date: 18/04/2014
Audience Size: 100k
Type and Goal Event: International Press Release about the ASPIRE project.
Countries Addresses: International

While the project started in Nov 2013, this press release was only released in April 2014 because it took a very long time to get the marketing departments of the project's industrial partners to agree on a text in which their principal investigators are quoted. Such quotations were preferred quite strongly, because or experience is that they make it much more likely that the press release is picked up by various news sites.
This news release was released via the Cordis Wire (http://cordis.europa.eu, published 17/4/2014) and AlphaGalileo (http://www.alphagalileo.org/ViewItem.aspx?ItemId=141251&CultureCode=en, published 25/04/2014). Moreover, we contacted our contact persons at ACM to ensure that the news was picked up by ACM TechNews, the most broadly spread news forum in the computing systems domain, reaching an audience of over hundred thousand readers. The press release was indeed picked up by ACM TechNews in its news bulletin of 25/04/2014 (http://technews.acm.org/archives.cfm?fo=2014-04-apr/apr-25-2014.html#720483).

8. Activity: Press Release
Main Leader: Bjorn De Sutter, UGent
Title: ASPIRE and Cyber Security
Date: 08/05/2014
Audience Size: -
Type and Goal Event: Short presentation of the ASPIRE project submitted to, and released by the European Cyber Security Round Table in their Cyber Newsflash.
Countries Addresses: International
URL: http://www.security-round-table.eu

9. Activity: Press Release
Main Leader: Bjorn De Sutter, UGent
Title: FP7 ASPIRE Project
Date: 07/2014
Audience Size: -
Type and Goal Event: Presentation of the project in the "In the Spotlight" section of HiPEAC info 39, the 39th issue of the newsletter of the FP7 HiPEAC Network of Excellence
Countries Addresses: International

URL: http://www.hipeac.net/content/hipeacinfo-39-july-2014

10. Activity: News Report on Television
Main Leader: Bjorn De Sutter, UGent
Title: Scuola anti pirati
Date: 30/07/2014
Audience Size: -
Type and Goal Event: A news report on local Italian television station TGVerona included fragments from Bjorn De Sutter's lecture on ASPIRE's software protection evaluation methodology. The whole report was 3.30 minutes long. See the screenshot in
Countries Addresses: Italy

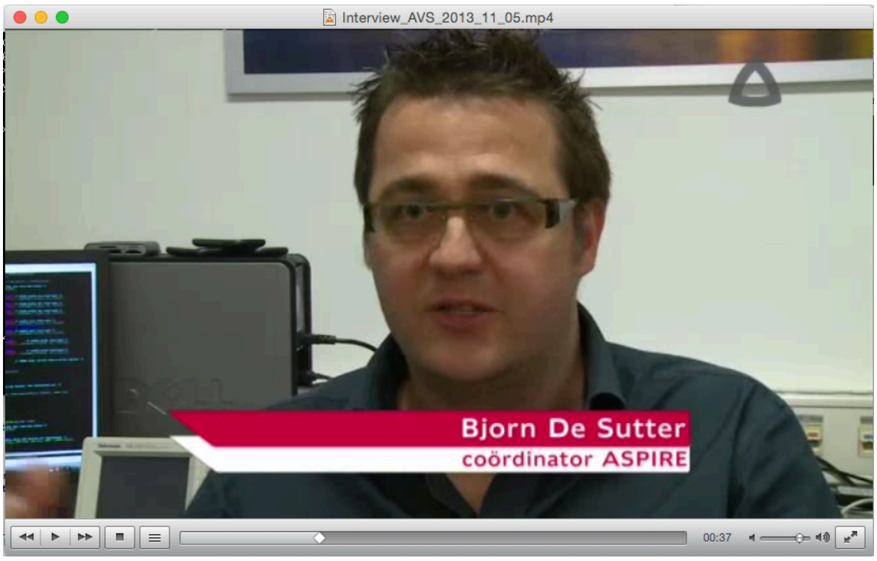


Figure 11 - Screenshot local television interview/report on AVS

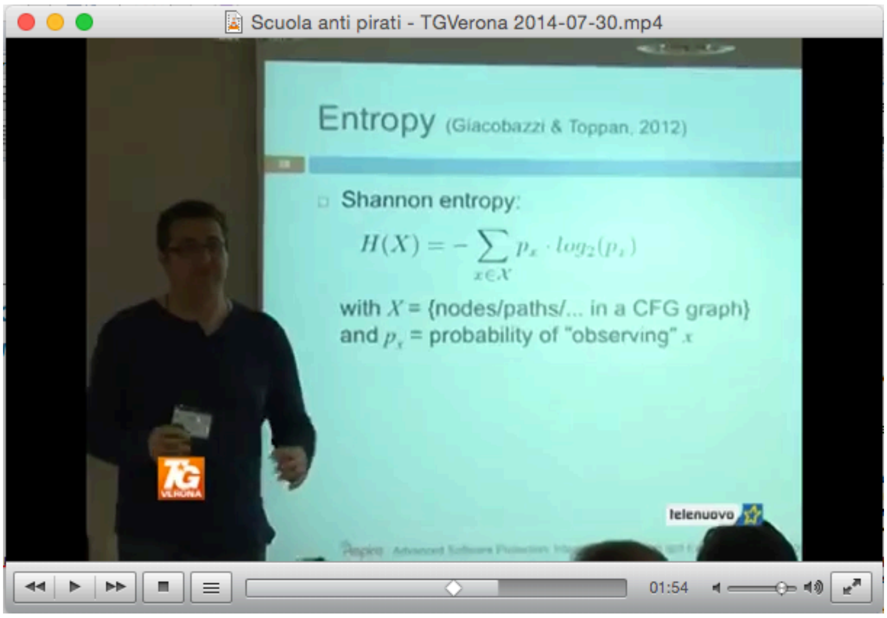

Scuola anti pirati - TGVerona 2014-07-30.mp4
Entropy (Giacobazzi & Toppan, 2012)
Shannon entropy:
$H(X) = -\sum_{x \in X} p_x \cdot log_2(p_x)$
with X = {nodes/paths/... in a CFG graph}
and p_x = probability of "observing" x
TG VERONA
telenuovo
01:54

Figure 12 - Screenshot local television report on TGVerona

2.4.2 Project Logo

To allow for a head start of the dissemination activities, the project coordinator launched a design contest "Create the next logo for ASPIRE" at the online design contest marketplace 99designs.com on 18 Sep 2013. In a process that lasted three weeks, 355 designs were submitted by about 40 designers. Initially the coordinator provided feedback on submitted designs himself, in later phases the ASPIRE Steering Board joined the selection process.

Eventually, the logo depicted in Figure 13 was selected:

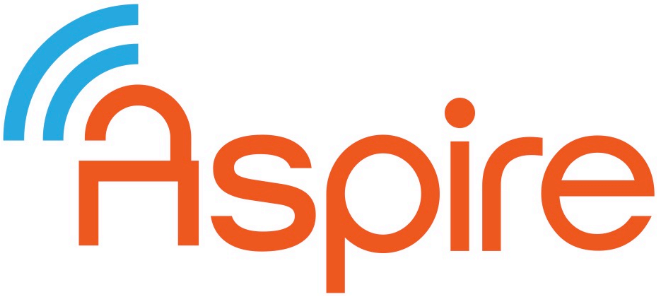


Figure 13 - ASPIRE logo

Along with that logo, the two buttons depicted in Figure 14 were delivered that can be used in all kinds of graphical disemmination material.

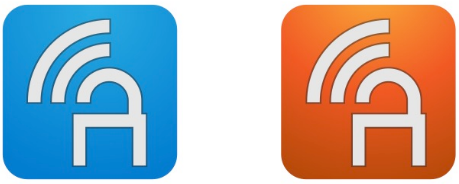
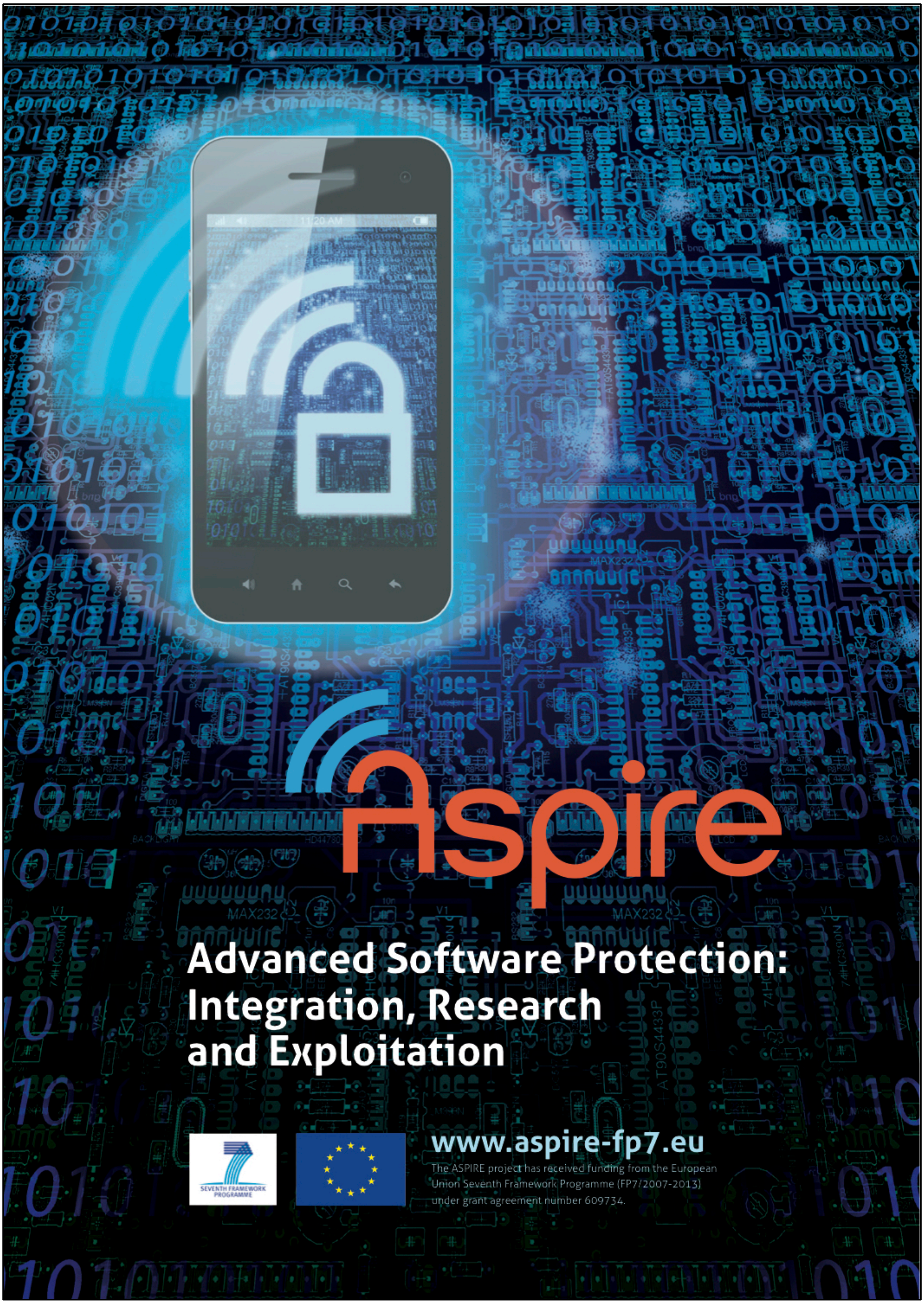


Figure 14 - ASPIRE buttons

2.4.3 Project Leaflet

As soon as the project had started, the communication company Magelaan (www.Magelaan.be) was hired to design a project leaflet that can be handed out by the project partners at networking events. Reduced quality versions of this 4-page A4 leaflet are shown in Figure 15 to Figure 18.

This flyer was distributed at multiple local and international events by multiple project partners.



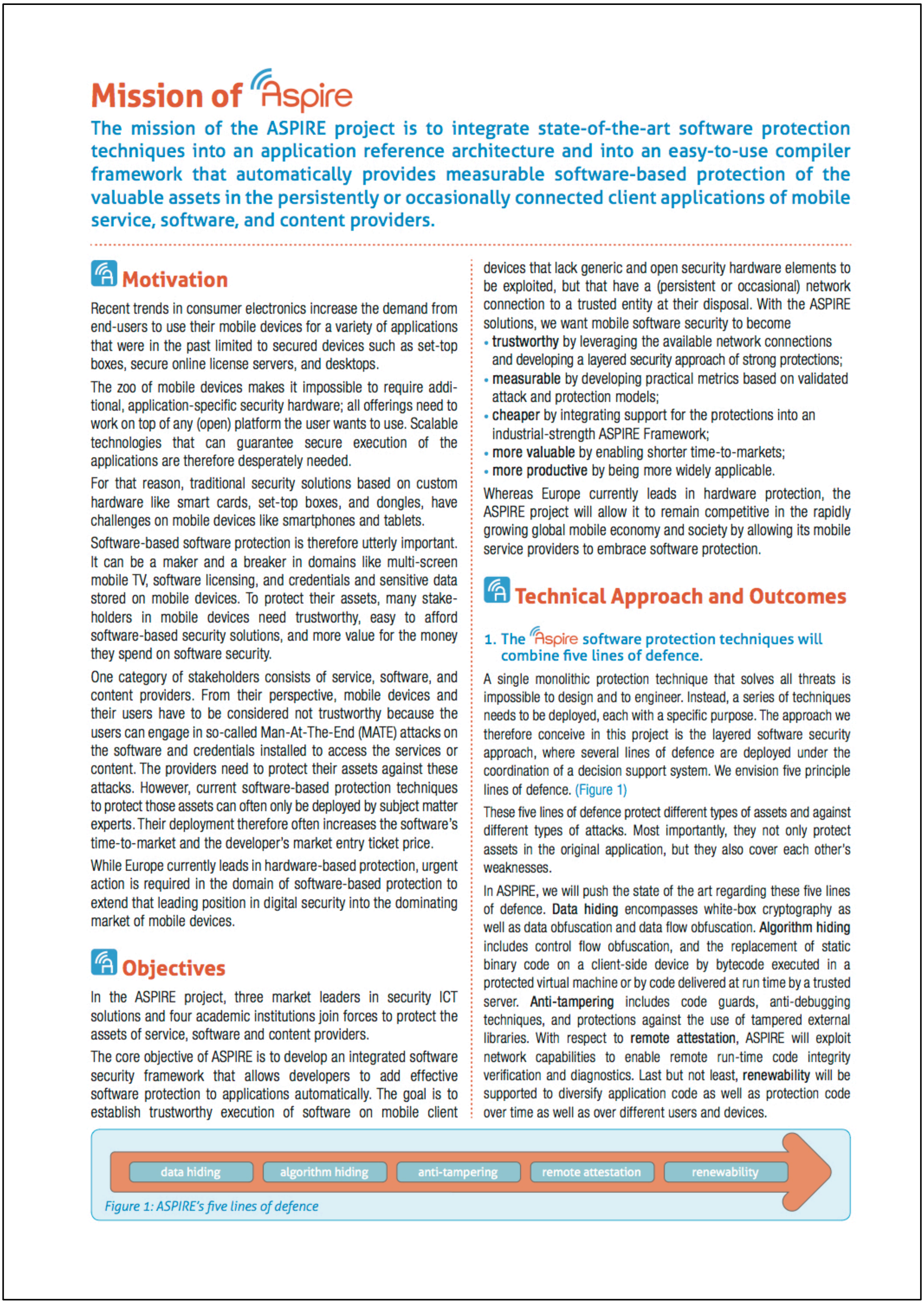
Aspire

Advanced Software Protection: Integration, Research and Exploitation

www.aspire-fp7.eu

The ASPIRE project has received funding from the European Union Seventh Framework Programme (FP7/2007-2013) under grant agreement number 609734.

Figure 15 - Front page ASPIRE leaflet



Mission of Aspire

The mission of the ASPIRE project is to integrate state-of-the-art software protection techniques into an application reference architecture and into an easy-to-use compiler framework that automatically provides measurable software-based protection of the valuable assets in the persistently or occasionally connected client applications of mobile service, software, and content providers.

Motivation

Recent trends in consumer electronics increase the demand from end-users to use their mobile devices for a variety of applications that were in the past limited to secured devices such as set-top boxes, secure online license servers, and desktops.

The zoo of mobile devices makes it impossible to require additional, application-specific security hardware; all offerings need to work on top of any (open) platform the user wants to use. Scalable technologies that can guarantee secure execution of the applications are therefore desperately needed.

For that reason, traditional security solutions based on custom hardware like smart cards, set-top boxes, and dongles, have challenges on mobile devices like smartphones and tablets.

Software-based software protection is therefore utterly important. It can be a maker and a breaker in domains like multi-screen mobile TV, software licensing, and credentials and sensitive data stored on mobile devices. To protect their assets, many stakeholders in mobile devices need trustworthy, easy to afford software-based security solutions, and more value for the money they spend on software security.

One category of stakeholders consists of service, software, and content providers. From their perspective, mobile devices and their users have to be considered not trustworthy because the users can engage in so-called Man-At-The-End (MATE) attacks on the software and credentials installed to access the services or content. The providers need to protect their assets against these attacks. However, current software-based protection techniques to protect those assets can often only be deployed by subject matter experts. Their deployment therefore often increases the software's time-to-market and the developer's market entry ticket price.

While Europe currently leads in hardware-based protection, urgent action is required in the domain of software-based protection to extend that leading position in digital security into the dominating market of mobile devices.

Objectives

In the ASPIRE project, three market leaders in security ICT solutions and four academic institutions join forces to protect the assets of service, software and content providers.

The core objective of ASPIRE is to develop an integrated software security framework that allows developers to add effective software protection to applications automatically. The goal is to establish trustworthy execution of software on mobile client devices that lack generic and open security hardware elements to be exploited, but that have a (persistent or occasional) network connection to a trusted entity at their disposal. With the ASPIRE solutions, we want mobile software security to become

- **trustworthy** by leveraging the available network connections and developing a layered security approach of strong protections;
- **measurable** by developing practical metrics based on validated attack and protection models;
- **cheaper** by integrating support for the protections into an industrial-strength ASPIRE Framework;
- **more valuable** by enabling shorter time-to-markets;
- **more productive** by being more widely applicable.

Whereas Europe currently leads in hardware protection, the ASPIRE project will allow it to remain competitive in the rapidly growing global mobile economy and society by allowing its mobile service providers to embrace software protection.

Technical Approach and Outcomes

1. The Aspire software protection techniques will combine five lines of defence.

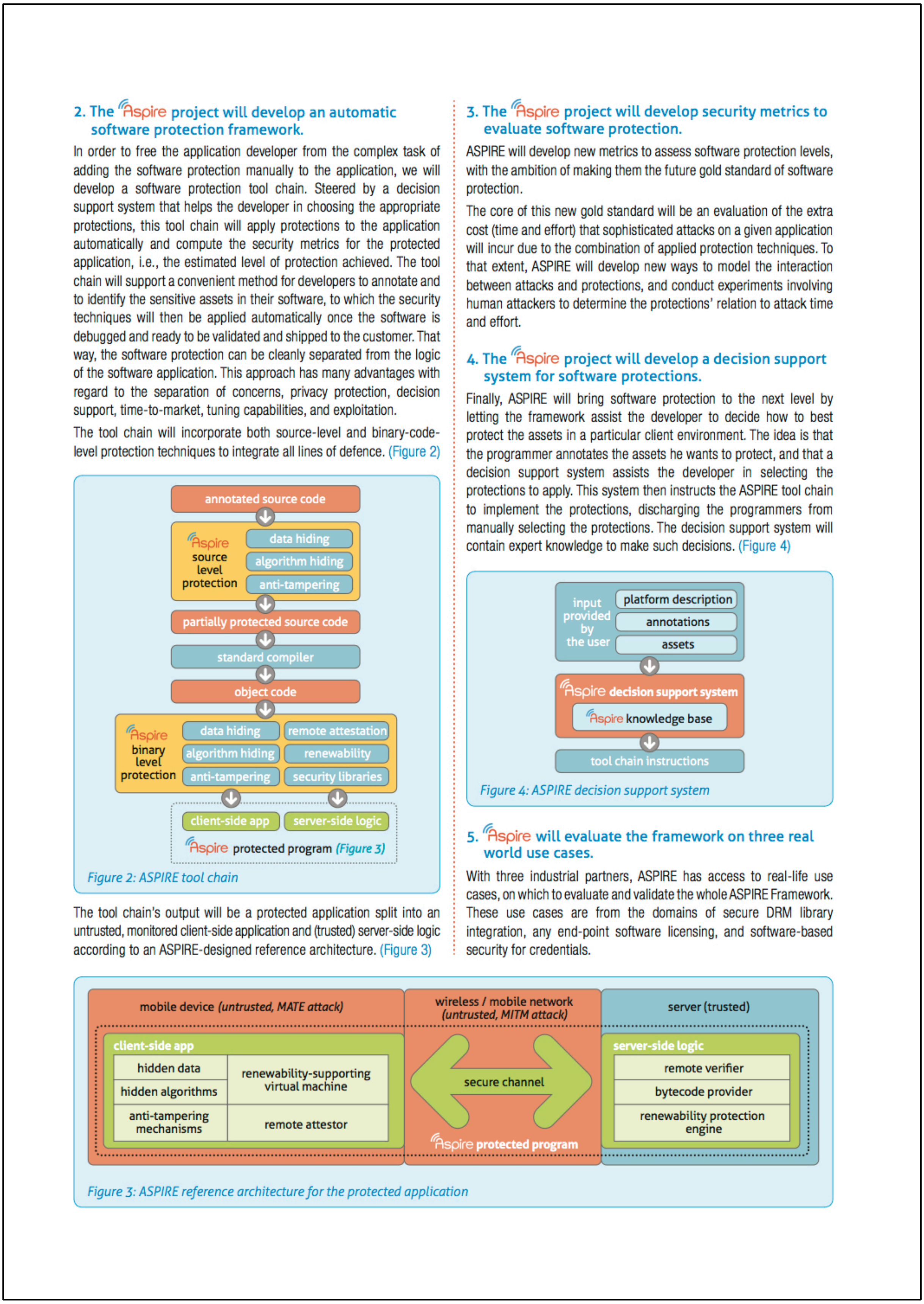
A single monolithic protection technique that solves all threats is impossible to design and to engineer. Instead, a series of techniques needs to be deployed, each with a specific purpose. The approach we therefore conceive in this project is the layered software security approach, where several lines of defence are deployed under the coordination of a decision support system. We envision five principle lines of defence. (Figure 1)

These five lines of defence protect different types of assets and against different types of attacks. Most importantly, they not only protect assets in the original application, but they also cover each other's weaknesses.

In ASPIRE, we will push the state of the art regarding these five lines of defence. **Data hiding** encompasses white-box cryptography as well as data obfuscation and data flow obfuscation. **Algorithm hiding** includes control flow obfuscation, and the replacement of static binary code on a client-side device by bytecode executed in a protected virtual machine or by code delivered at run time by a trusted server. **Anti-tampering** includes code guards, anti-debugging techniques, and protections against the use of tampered external libraries. With respect to **remote attestation**, ASPIRE will exploit network capabilities to enable remote run-time code integrity verification and diagnostics. Last but not least, **renewability** will be supported to diversify application code as well as protection code over time as well as over different users and devices.

Figure 1: ASPIRE's five lines of defence

Figure 16 - Page 2 ASPIRE leaflet



2. The Aspire project will develop an automatic software protection framework.

In order to free the application developer from the complex task of adding the software protection manually to the application, we will develop a software protection tool chain. Steered by a decision support system that helps the developer in choosing the appropriate protections, this tool chain will apply protections to the application automatically and compute the security metrics for the protected application, i.e., the estimated level of protection achieved. The tool chain will support a convenient method for developers to annotate and to identify the sensitive assets in their software, to which the security techniques will then be applied automatically once the software is debugged and ready to be validated and shipped to the customer. That way, the software protection can be cleanly separated from the logic of the software application. This approach has many advantages with regard to the separation of concerns, privacy protection, decision support, time-to-market, tuning capabilities, and exploitation.

The tool chain will incorporate both source-level and binary-code-level protection techniques to integrate all lines of defence. (Figure 2)

Figure 2: ASPIRE tool chain

The tool chain's output will be a protected application split into an untrusted, monitored client-side application and (trusted) server-side logic according to an ASPIRE-designed reference architecture. (Figure 3)

3. The Aspire project will develop security metrics to evaluate software protection.

ASPIRE will develop new metrics to assess software protection levels, with the ambition of making them the future gold standard of software protection.

The core of this new gold standard will be an evaluation of the extra cost (time and effort) that sophisticated attacks on a given application will incur due to the combination of applied protection techniques. To that extent, ASPIRE will develop new ways to model the interaction between attacks and protections, and conduct experiments involving human attackers to determine the protections' relation to attack time and effort.

4. The Aspire project will develop a decision support system for software protections.

Finally, ASPIRE will bring software protection to the next level by letting the framework assist the developer to decide how to best protect the assets in a particular client environment. The idea is that the programmer annotates the assets he wants to protect, and that a decision support system assists the developer in selecting the protections to apply. This system then instructs the ASPIRE tool chain to implement the protections, discharging the programmers from manually selecting the protections. The decision support system will contain expert knowledge to make such decisions. (Figure 4)

Figure 4: ASPIRE decision support system

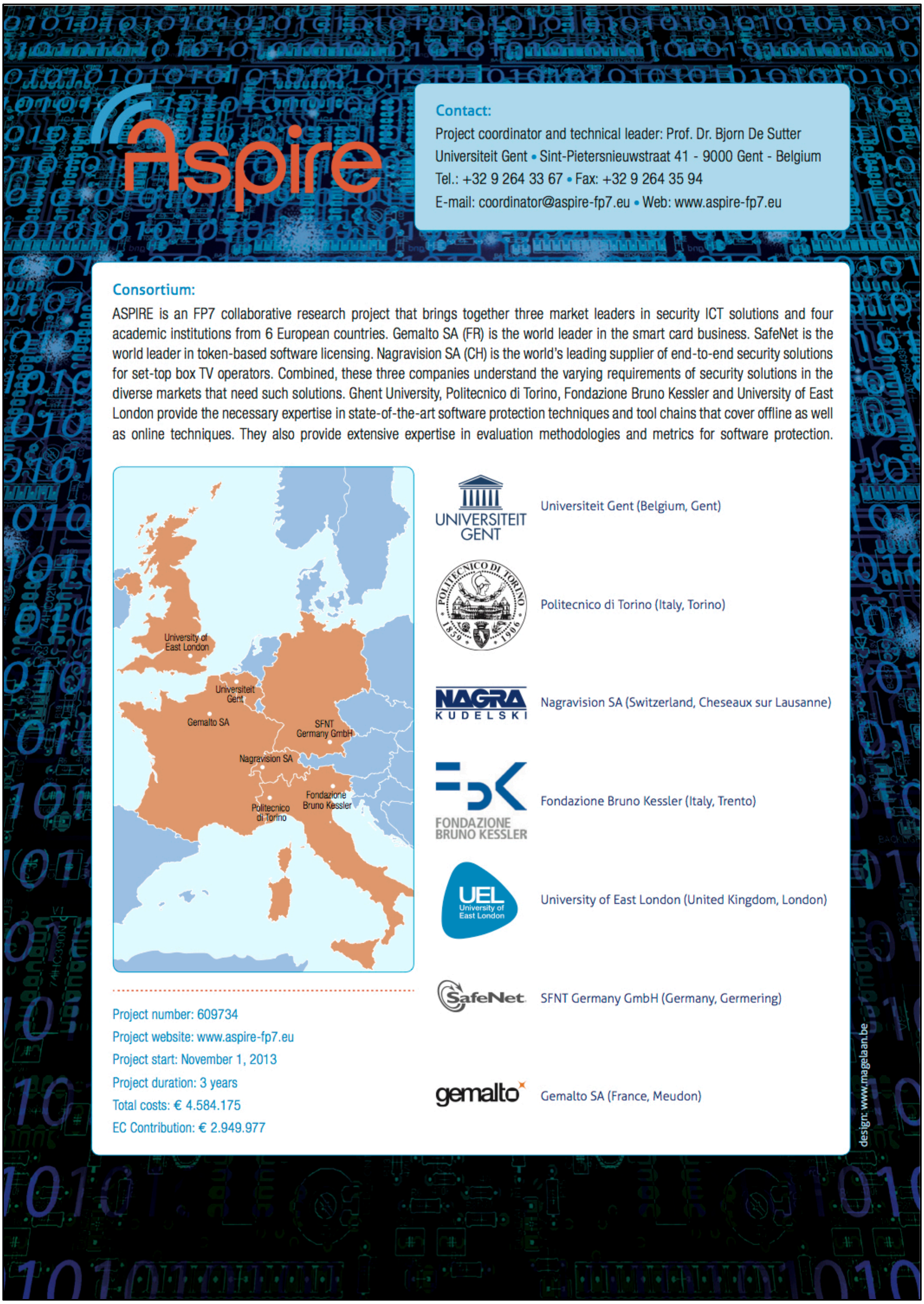
5. Aspire will evaluate the framework on three real world use cases.

With three industrial partners, ASPIRE has access to real-life use cases, on which to evaluate and validate the whole ASPIRE Framework. These use cases are from the domains of secure DRM library integration, any end-point software licensing, and software-based security for credentials.

mobile device (untrusted, MATE attack)
wireless / mobile network (untrusted, MITM attack)
server (trusted)
client-side app
hidden data
hidden algorithms
renewability-supporting virtual machine
anti-tampering mechanisms
remote attestor
secure channel
Aspire protected program
server-side logic
remote verifier
bytecode provider
renewability protection engine

Figure 3: ASPIRE reference architecture for the protected application

Figure 17 - Page 3 ASPIRE leaflet



Contact:

Project coordinator and technical leader: Prof. Dr. Bjorn De Sutter
Universiteit Gent • Sint-Pietersnieuwstraat 41 - 9000 Gent - Belgium
Tel.: +32 9 264 33 67 • Fax: +32 9 264 35 94
E-mail: coordinator@aspire-fp7.eu • Web: www.aspire-fp7.eu

Consortium:

ASPIRE is an FP7 collaborative research project that brings together three market leaders in security ICT solutions and four academic institutions from 6 European countries. Gemalto SA (FR) is the world leader in the smart card business. SafeNet is the world leader in token-based software licensing. Nagravision SA (CH) is the world's leading supplier of end-to-end security solutions for set-top box TV operators. Combined, these three companies understand the varying requirements of security solutions in the diverse markets that need such solutions. Ghent University, Politecnico di Torino, Fondazione Bruno Kessler and University of East London provide the necessary expertise in state-of-the-art software protection techniques and tool chains that cover offline as well as online techniques. They also provide extensive expertise in evaluation methodologies and metrics for software protection.

Universiteit Gent (Belgium, Gent)

Politecnico di Torino (Italy, Torino)

Nagravision SA (Switzerland, Cheseaux sur Lausanne)

Fondazione Bruno Kessler (Italy, Trento)

University of East London (United Kingdom, London)

SFNT Germany GmbH (Germany, Germering)

Gemalto SA (France, Meudon)

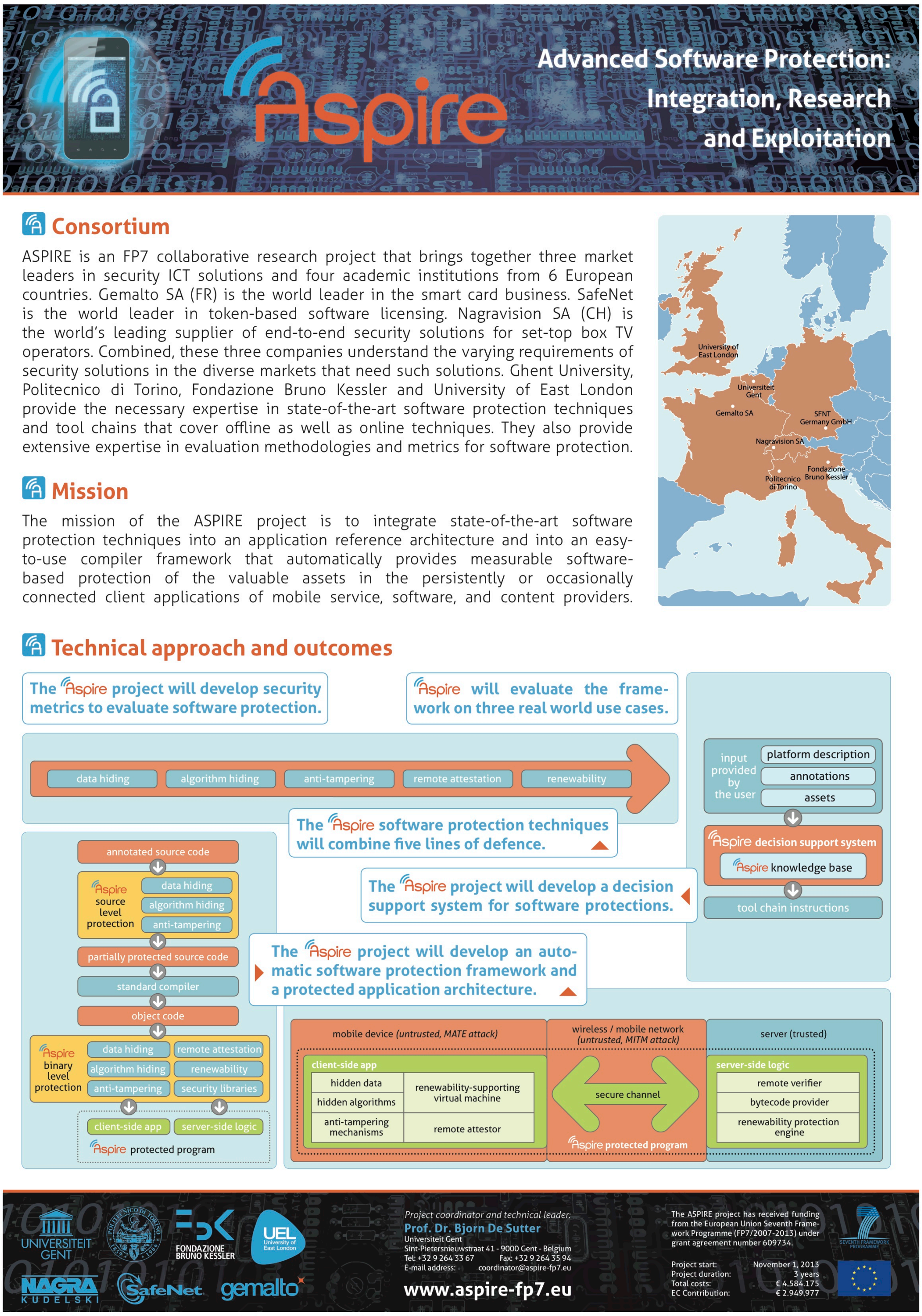
Project number: 609734
Project website: www.aspire-fp7.eu
Project start: November 1, 2013
Project duration: 3 years
Total costs: € 4.584.175
EC Contribution: € 2.949.977

design: www.magelaan.be

Figure 18 - Back page ASPIRE leaflet

2.4.4 Project Poster

On the basis of the project leaflet graphics, we also designed (internally) a general ASPIRE poster that can be reused by all partners at poster events. This A0-poster is depicted in Figure 19 at reduced resolution.



Advanced Software Protection: Integration, Research and Exploitation

Consortium

ASPIRE is an FP7 collaborative research project that brings together three market leaders in security ICT solutions and four academic institutions from 6 European countries. Gemalto SA (FR) is the world leader in the smart card business. SafeNet is the world leader in token-based software licensing. Nagravision SA (CH) is the world's leading supplier of end-to-end security solutions for set-top box TV operators. Combined, these three companies understand the varying requirements of security solutions in the diverse markets that need such solutions. Ghent University, Politecnico di Torino, Fondazione Bruno Kessler and University of East London provide the necessary expertise in state-of-the-art software protection techniques and tool chains that cover offline as well as online techniques. They also provide extensive expertise in evaluation methodologies and metrics for software protection.

Mission

The mission of the ASPIRE project is to integrate state-of-the-art software protection techniques into an application reference architecture and into an easy-to-use compiler framework that automatically provides measurable software-based protection of the valuable assets in the persistently or occasionally connected client applications of mobile service, software, and content providers.

Technical approach and outcomes

The Aspire project will develop security metrics to evaluate software protection.

Aspire will evaluate the framework on three real world use cases.

The Aspire software protection techniques will combine five lines of defence.

The Aspire project will develop a decision support system for software protections.

The Aspire project will develop an automatic software protection framework and a protected application architecture.

Project coordinator and technical leader:
Prof. Dr. Bjorn De Sutter
Universiteit Gent
Sint-Pietersnieuwstraat 41 - 9000 Gent - Belgium
Tel: +32 9 264 33 67 Fax: +32 9 264 35 94
E-mail address: coordinator@aspire-fp7.eu
www.aspire-fp7.eu

The ASPIRE project has received funding from the European Union Seventh Framework Programme (FP7/2007-2013) under grant agreement number 609734.

Project start:	November 1, 2013
Project duration:	3 years
Total costs:	€ 4.584.175
EC Contribution:	€ 2.949.977

Figure 19 - ASPIRE poster

2.4.5 Social Media

Social media can help in spreading project-related information to a wide audience. They are therefore a valuable tool to disseminate project ideas and results. To start using social media, we waited until enough results were becoming available, such that we can avoid so-called sleeping social media accounts.

In September 2014, the ASPIRE FP7 **Twitter** account was launched (https://twitter.com/aspirefp7), where project members can tweet about the project and related subjects.

In November 2014, the ASPIRE FP7 **LinkedIn** group was launched (https://www.linkedin.com/groups/Aspire-FP7-7300827), where stakeholders and other interested people will be able to get connected, and where we will disseminate project results.

2.4.6 Cooperation with Other Projects

UGent collaborated with the TETRACOM FP7 project (http://www.tetracom.eu) to further prepare its IP for exploitation by an industrial partner, as documented more extensively in deliverable D7.03.

UGent's ASPIRE team also provides input to the vision building processes in the HiPEAC Network of Excellence (http://www.hipeac.net), in particular for drafting the HiPEAC vision documents and roadmaps on compiler technology and their use for protecting and securing software and computer systems.

Furthermore, the project coordinator is active in the Digital Asset Protection Association (DAPA) project/organization (http://www.digitalassetprotectionassociation.org/), where he is working with the scientific board members to draft a whitepaper on best practices for publishing and evaluation software protection papers and results. That work is of course heavily influenced by the methodology developed in WP4 of the ASPIRE project.

Within Torino, there is a collaboration between the ASPIRE researchers and the researchers of the SECURED project. The SECURED project needs to remotely attest the software that has to execute the user security application. Currently, the preferred approach is the TCG-based one, which uses secure hardware, i.e., the TPM, as root core of trust. After the remote attestation result will be available, the SECURED group will consider the ASPIRE-proposed software-only approach. Additionally, the software protection techniques can be used to mitigate the risks against the SECURED app, the piece of software running on the user terminals in charge for communicating with the SECURED infrastructure and the user security application execution environments.

Nagravision participates to the Celtic-plus project (http://celticplus.eu/) on HEVC Hybrid Broadcast Video Services (H2B2VS, http://h2b2vs.epfl.ch). That project investigates the hybrid distribution of TV programs and services over heterogeneous networks. H2B2VS impacts requirements Nagravision puts forward for ASPIRE technology. Vice versa, ASPIRE uncovers options to securely deploy heterogeneous end devices as targeted by H2B2VS.

2.4.7 Interview for EU Yearbook

Based on an interview with the project Coordinator (taken on 30 April 2014), an article about the ASPIRE project will be published in the EU Yearbook, which will be compiled by the team of the EU FP7 project SecCord (http://www.seccord.eu). This article is yet another way of making the public community aware of ASPIRE.

Section 3 Global Dissemination Plan Years 2 - 3

Section Authors:

Bjorn De Sutter (UGent)

In year 2 and 3, the project shifts from the awareness phase to the result phase and eventually the exploitation phase of the project results. In line with, and in addition to the activities mentioned in the dissemination strategy in Section 1.1, the major dissemination activities in those years will be

1. the continuous updating of the website, incl. the publication of project deliverables;
2. the submission of many collaborative papers to conferences by the consortium partners;
3. press releases following major milestones being reached;
4. presence at major European networking and dissemination events;
5. two workshops and a tutorial.

For the submission of papers, we refer to the publication venues listed in Section 1.1, as well as additional venues mentioned in the individual partners' dissemination plans presented in Section 4.

Regarding the presence at major European networking events, the project will strive for greater presence and visibility than during the first year. In particular, the coordinator will attend the CSP Forum Conference in 2015. The coordinator has already contacted CSP Forum to ensure that, unlike in 2014, the ASPIRE internal review does not accidentally overlap with the CSP Forum Conference.

A major update to the dissemination strategy is that instead of organizing one workshop, the ASPIRE consortium will try organize two or more workshops and tutorials. The reason is that different aspects of the ASPIRE project relate to different communities. To reach those different communities, multiple events are necessary.

As mentioned in the above strategy, the original goal was to organize a workshop collocated with one of the major networking events, i.e., conferences, in Europe. As a consequence of the collocation, a workshop proposal needs to be created and submitted to the events' calls for workshops. In other words, the decision to organize the workshop or not is not fully controlled by the ASPIRE consortium itself.

One workshop proposal has been prepared and submitted to the International Conference on Software Engineering (ICSE) 2015. See Section 2.2.4 and Appendix A for more details. The workshop selection process at ICSE is quite competitive, but on 20 November 2014 we got notification that the workshop was indeed accepted. So this will provide an excellent opportunity to interact with and disseminate to the software engineering community.

A second workshop proposal will be submitted to the HiPEAC 2016 Conference. The acceptance rate there is higher, and UGent organizes the main conference, so we trust that the proposal will effectively be accepted. Through such a workshop, we will reach the compiler research community.

In addition we propose to organize one or more tutorials on ASPIRE technology. These will be organized towards the end of the project, or even after the project has ended, when the technology has reached enough maturity to include hands-on sessions.

Section 4 Per Partner Dissemination Plans

Section Authors:

Bjorn De Sutter (UGent), Mariano Ceccato (FBK), Cataldo Basile (POLITO), Michael Zunke (SFNT), Jerome D'Annovile (GTO), Brecht Wyseur (NAGRA), Paolo Falcarin (UEL)

In Appendix B7 of the DoW - Annex I Part B, all ASPIRE consortium partners already briefly presented their dissemination plans. In this section, we extend those presentations. In this section, italic text is copied from the DoW - Annex I Part B Appendix B7.

4.1 Ghent University

UGent plans to publish the main results of the project to which it contributes in the scientific publication venues mentioned in Section B3.2.1 of the DoW.

As its core research domain is compiler technology, it will also publish results in compiler-oriented publication venues such as DAC, DATE, CGO, PLDI, LCTES, CC, the HiPEAC conference, TACO and TOPLAS.

Concretely, and as first and lead author, UGent/CSL is planning to write and to submit papers on the following topics:

- ASPIRE software protection metric framework (task T4.2 - 2-3 papers);
- existing binary code control flow obfuscations and their potential to thwart reverse-engineering tools such as IDA Pro for ARM code (task T2.4 - 1 paper);
- advanced control flow obfuscations based on two-way predicates and complex data structures for encoding predicate values (task 2.4 - 1-2 papers);
- the anti-debugging technique (task T2.5, 1-2 papers);
- strategies for choosing code splitting points to obfuscate control flow (tasks T2.3 and T3.1);
- the public challenge (task T5.3).

As potentially first author, but not necessarily so, UGent also plans to write and to submit papers on all other aspects of the project to which it contributes, i.e., almost all aspects.

As coordinator of the project, UGent has already proposed to make additional existing deliverables public, such as deliverable D1.02, after its content has been revised and condensed into a paper. The consortium has agreed with this.

Near the end of the project, the coordinator will take the initiative to write a book that brings together all ASPIRE results.

UGent will also participate in all awareness-oriented and research-oriented dissemination activities mentioned in Section 1.1, in particular in the ISSISP summer school that it co-organizes and at which it lectures.

In July 2014, the project coordinator already gave a lecture on software protection evaluation at ISSISP 2014 in Verona. For 2015 and 2016, potential countries for hosting the summer school are Armenia and Brazil. The project coordinator is involved in the choice and determination of the program.

As coordinator and face of the ASPIRE project, UGent will actively promote the project at related networking events and take part in the exploitation-oriented activities where useful.

In 2014, this included a so-called Dagstuhl seminar (Dagstuhl Seminar 14241 on Challenges in Analysing Executables: Scalability, Self-Modifying Code and Synergy, June 9–13, 2014), and the ARO Workshop on Continuously Upgradeable Software Security and Protection, Jun 7, 2014. In addition, the project coordinator gave a keynote speech at the First Workshop on Cryptography and Security in Computing Systems, Jan 20, 2014. Similar activities will be taken up during year 2 and 3 of the project, and after the project has finished.

In 2015 and 2016, the coordinator will also participate more actively in CSP Forum activities.

The main achievements with Diablo are also published on the Diablo website.

In due time, and as allowed by the commercial licensing agreements between CSL and industrial third parties, UGent plans to open-source all of the extensions developed in ASPIRE in and on top of its Diablo link-time framework. At that time, the Diablo (diablo.elis.ugent.be) website will also be revamped, to put additional emphasis on the big steps forward realized in the ASPIRE project.

As software protection is a prime example of compiler and system software technology, UGent also plans to use all the available means of the HiPEAC3 Network of Excellence, which is coordinated by UGent, to disseminate the results to the European compiler & computer architecture research community.

At the HiPEAC 2015 conference, the coordinator will present two posters. A first one will be presented at the TETRACOM workshop collocated with the conference. This will present the successful technology transfer to Samsung Research UK. The second one will present the project at the HiPEAC 2015 General Poster Session.

Also at future so-called Computing System Weeks, organized by HiPEAC, ASPIRE results will be presented.

As the HiPEAC conference is organized by the administrative personnel that also supports the ASPIRE management activities within UGent/CSL, UGent will take the lead in organizing the HIPEAC workshop to be collocated with HiPEAC 2016.

In addition to the aforementioned, UGent will also take up its responsibilities with regard to the maintenance and extension of the ASPIRE website as a knowledge base on relevant work in the domain of ASPIRE.

Finally, UGent plans to let students perform their master thesis research in the context of ASPIRE. For the academic year 2014-2015, three students have already started their research, on topics in the domains of (1) software protections of Windows applications based on static linking, (2) advanced opaque predicates, and (3) anti-debugging techniques. All three are progressing well, so we expect to publish their master theses in June 2015. For the academic year 2015-2016, we will submit a new round of research project proposals for in March 2015.

4.2 Politechnico Di Torino

POLITO plans to submit results of security evaluation to top journals and conferences on software engineering and security, as mentioned in Section B3.2.1 of the DoW. POLITO will also contribute to the dissemination of ASPIRE results at European level, and to foster collaboration with other EU funded project. A special role will have the participation to EU coordination activities, such as the current EffectPlus events and clusters.

Concretely, and as first and lead author, POLITO is planning to write and to submit papers on the following topics:

- *Software Protection,* we expect important publishable results in a novel field of remote attestation that we are designing in this phase of the project, the Implicit Remote Attestation.

- *Security model,* we expect a number of publications in software risk analysis and mitigation models, from the work to build the ASPIRE Knowledge Base (AKB), as presently, there is no model of the software protection ecosystem in literature that can be compared to the AKB on accuracy and expressiveness
- *Ontology-based enrichment framework*, we expect important publishable results from the ASPIRE Enrichment Framework in task T5.2 in the ontology and formal methods field.
- *Decision support and software protection optimization models,* we expect a number of publications from the work on the decision of the "best" combination of protections to protect the application assets is a new idea that we plan to publish as soon as the ADSS results will be mature.
- *Empirical assessment of software protection*, we expect a number of publications from the results of the empirical evaluation of protections with academic and industrial participants.

As potentially the first author, but not necessarily so, POLITO also plans to write and to submit papers on all other aspects of the project to which it contributes, which are mainly related to WP3, WP4, and WP5 aspects.

Dissemination of project results will be also conducted within the Politecnico di Torino, by presenting the objectives of the project in the course of "Sicurezza dei sistemi informatici" and "Computer system security", having Antonio Lioy and Cataldo Basile as teachers. Moreover, we plan to have 5-10 thesis at the end of the three years of the project, presenting small and focused innovations conducted within the ASPIRE project.

POLITO will also continue dissemination:

- Internal, within the Politecnico, by presenting the ASPIRE project and ASPIRE results to other research groups, that may be also involved other EU proeject
- External, by participating to conferences, workshops, and EffectPlus and other EU events, and
- External, by disseminating ASPIRE goals and results on national media.

4.3 Nagravision

As for the result phase of the dissemination, NAGRA aims to establish public credibility by publishing new results at top-level conferences such as EUROCRYPT, CRYPTO, CHES, CARDIS, DRM, ESORICS; publish corporate white-papers and articles for journals. NAGRA employees are often also speakers at relevant events, which enables evangelisation.

In addition, NAGRA has several tracks of dissemination planned. This includes both internal dissemination as external dissemination of ASPIRE results.

As for internal dissemination, this includes

- Frequent publication of ASPIRE results and project progress on an internal blog,
- Presentation of the project results at security workshops, in particular "security deep dives". This is a special series of workshops that is organized every 6 months in which the Kudelski Group security experts gather to discuss and disseminate various security topics. The Principal Investigator of NAGRA to the ASPIRE project is a frequent speaker at this workshop and has presented about the project in the past editions. This dissemination will continue in the next editions.

Results of the ASPIRE project will be further disseminated to software developers and architects in NAGRA's business units. This has for example already been done for the demonstrator that has been developed in WP6.

As for the exploitation phase of the dissemination, NAGRA will also participate to tradeshows with its products that are protected with the ASPIRE tool chain; in particular, we shall expose the project results at our booth at IBC (the yearly International Broadcasting Convention) and participate to CES (the yearly Consumer Electronics Show).

For further external dissemination, NAGRA envisions two main tracks.

1. To disseminate towards business audience, aiming directly to attract new customers by demonstrating technology. This can be achieved by demonstrating ASPIRE-based technology and products at tradeshows such as IBC (the yearly International Broadcasting Convention) or CES (the yearly Consumer Electronics Show), which are the main events in our market segment. This is planned for towards the end of the ASPIRE project, when the results become mature enough for presentation.
2. To establish credibility by publishing new results and showing our participation to the ASPIRE project. This targets a more research-oriented community, with publications and conferences and workshops of relevance. In the first year of the project, NAGRA employees have been presenting about ASPIRE at scientific events, as shown in the list in Section 2, and NAGRA plans to continue to support such activities.

4.4 Fondazione Bruno Kessler

FBK plan to submit results of security evaluation to top journals and conferences on empirical software engineering, as mentioned in Section B3.2.1 of the DoW.

Concretely, and as first and lead author, FBK is planning to write and to submit papers on the following topics:

- Implementation and assessment of data obfuscation based on state-of-the-art approaches, e.g. residue number coding (Task T2.1);
- Improvement and extensions of state-of-the-art data obfuscation approaches, towards more secure solutions that are more resilient to static analysis (Task T2.1);
- Client-server code splitting based on barrier slicing and its performance assessment (Task T3.1);
- Source code level software metric to measure the impact of software protection approaches (task T4.2);
- Design, results, discussion and interpretation of the results of the controlled experiments devoted to assess software protection with academic participants (Task T4.3) and with industrial participants (Task T4.4).

As potentially the first author, but not necessarily so, FBK also plans to write and to submit papers on other topics of the project to which it contributes:

- Presentation of the state of the art attacks on software integrity for the definition of a comprehensive attack model (Task T1.4);
- Code diversity and heuristics to search in the search space for the most “diverse” versions to deploy with updates (Task T3.3);
- Design and results, discussion and interpretation of the public challenge (Task T4.5).

Dissemination of project results will be also conducted by presenting the objectives of the project in the course of “Security Testing” that Paolo Tonella and Mariano Ceccato teach in the Master Degree in Computer Science in the University of Trento.

Moreover, small and well-defined activities will be identified in the tasks lead by FBK, to be assigned as master theses to master students. As such, students involved in master theses related to the project will be required to spend some time to familiarize with the specific context of ASPIRE. With the help of the thesis supervision, the master student will elaborate, implement and assess a small and novel contribution that fits the objective of the project. As a matter of fact, this strategy was already successful adopted in the first year of the project, as demonstrated by the theses listed in Section 2.1.

4.5 University of East London

UEL plans to publish the main results of the project to which it contributes in the scientific publication venues mentioned in Section B3.2.1 of the DoW.

UEL will coordinate the dissemination activities in ASPIRE project and next to the ASPIRE workshop, UEL will co-organize workshops on software protection collocated with important international conferences in software engineering (ICSE) and security (CCS).

Concretely, and as first and lead author, UEL is planning to write and to submit papers on the following topics:

- *Code Mobility as Software Protection,* we expect important publishable results in the novel field of network-based protections based on code mobility, and dynamic renewability of code.
- Code diversity and heuristics to search in the search space for the most “diverse” versions to deploy with updates (Task T3.3);
- Extension of code mobility with UGent's Diablo binary rewriter (T3.1);
- Extension of code mobility with SafeNet's VM on Android (T3.1);
- *Security model,* we expect a number of publications on Petri-nets attack models and related toolset, as presently, there is no model of the software protection attacks in literature and no tools to evaluate them.

As potentially the first author, but not necessarily so, UEL also plans to write and to submit papers on all other aspects of the project to which it contributes (in WP3, WP4, and WP5).

In particular, UEL wants to contribute to the following activities:

- Presentation of the state of the art attacks on software protection for the definition of a comprehensive attack model (Task T1.4), with particular focus on network-based protections;
- Extension of code mobility with remote attestation (Tasks T3.1 and T3.2).
- Construction of the ASPIRE Knowledge Base (AKB) by adding and extracting attack models (Task T4.1 and T5.2);
- *Decision support and software protection optimization models*: decision of the “best” combination of protections to protect the application assets;
- *Empirical assessment of software protection*, we expect a number of publications from the results of the empirical evaluation of protections with academic and industrial participants.

UEL and NAGRA will co-organize a workshop on software protection accepted as collocated event with the International Conference in Software Engineering (ICSE-2015) in May 2015.

UEL will lead the workshop organization, setting up the Program Committee, advertising the call for papers and organizing the papers review among the PC members.

Dissemination of project results will be also conducted within UEL, by presenting the objectives of the project in the modules of "Programming Languages" and “Computer security”, having Paolo Falcarin and Christophe Tartary as lecturers. Moreover, we plan to have 3-10 overall undergrad and postgrad final thesis at the end of the three years of the project, presenting small and focused innovations performed during the ASPIRE project.

UEL will also continue dissemination:

- Internal, by presenting the ASPIRE project results to other research groups;
- External, by participating to conferences, workshops, and other EU events.

4.6 SFNT Germany

During the results phase SFNT will market the participation and results through its marketing channels including press releases where applicable.

Once promising results of the ASPIRE metric are available and SFNT can show its value the metric is expected to be used to classify protections in order to start educating the market about efficient protections. Internally product enhancements will be guided by the metrics. To prepare for this the project is promoted internally to the Senior System Architects and the respective product owners. Discussion with the product owners already have started and feedback to development is expected to start as soon as positive results are achieved.

For the exploitation phase SFNT will promote the metrics developed in ASPIRE in its products and in relevant developer conferences. This includes participation in trade shows and press releases about it.

The metric could be introduced to the SIIA and might influence the way how security solutions will get judged towards the well-known Codie Awards.

4.7 Gemalto

A first action is to disseminate ASPIRE results within the Gemalto company. Several internal workshops will be organized during the last year of the project and demonstrations of the protection techniques are demonstrated to Software developers in Business Units in order to collect feedbacks. These feedbacks will contribute to define the Gemalto ASPIRE product. The target teams identified so far are the eBanking teams.

As the external dissemination activity, Gemalto intends to rely on existing connections settled in a Living Lab.

Finland initiated the concept of Living Lab in 2006 with the idea to gather users, researchers and implementers in an experiential environment where the user is associated in the creation process. It is mainly IT focussed but it has a broader spectrum. There are more than 300 Living Labs in Europe. It is oriented on experimentations with users to assess innovations not to test alpha/beta releases of products but to induce the product definition. Participants to this ecosystem are located in the same geographical area that can be a city or a region.

The Secure Electronic Transactions cluster (TES acronym in French) is part of the French Normandy Living Lab (NLL). It is focussed on the three main topics: contactless payment, eCitizen and eAdministration. Experiment has been conducted in 2005 (“Caen ville NFC”) and in 2008 on payment with mobile device. Gemalto is member of TES.

The plan is to be active in this cluster by proposing a concrete experimentation about contactless mobile payment based on applications secured by ASPIRE. From M24, some tangible protections can be proposed to members of the cluster. The motivation of this cooperation is to define the Gemalto ASPIRE product and the expected results are feedback on the ACTC, the protection configuration, tools would be required to assist application developers in the source code annotation activity, ADSS assessment, reports convenience, ...

Section 5 List of Abbreviations

ACM	Association of Computing Machinery
ARO	Army Research Office
ASPIRE	Advanced Software Protection: Integration, Research and Exploitation
CARDIS	Smart Card Research and Advanced Application Conference
CC	Compiler Construction
CCS	Computer and Communications Security
CGO	Code Generation and Optimization
CHES	Cryptographic Hardware and Embedded Systems
CRYPTO	Cryptology
CSL	Computer Systems Lab
CSP	Cyber Security & Privacy
DAC	Design Automation Conference
DAPA	Digital Asset Protection Association
DATE	Design, Automation & Test in Europe
DoW	Description of Work
DRM	Digital Rights Management
ESORICS	European Symposium on Research in Computer Security
EU	European Union
EUROCRYPT	Annual International Conference on the Theory and Applications of Cryptographic Techniques
H2B2VS	HEVC Hybrid Broadcast Video Services
HiPEAC	High Performance and Embedded Architecture and Compilation
IEEE	Institute of Electrical and Electronics Engineers
ICSE	International Conference on Software Engineering
IT	Information Technology
LCTES	Languages, Compilers, Tools and Theory for Embedded Systems
NFC	Near Field Communication
NLL	Normandy Living Lab
PLDI	Programming Language Design and Implementation
RA	Remote Attestation
SECURED	SECURity at the network EDge
SIIA	Software & Information Industry Association
TACO	Transactions on Architecture and Code Optimization
TES	Secure Electronic Transactions (Transactions Electroniques Securisées in French)
TETRACOM	Technology Transfer in Computing Systems
TCG	Trusted Computing Group
TOPLAS	Transactions on Programming Languages and Systems
TORSEC	Torino Security
TPM	Trusted Platform Module
WP	Work Package

Appendix A First ASPIRE Workshop Proposal

Software Protection Workshop

Security Evaluation and Industrial Best Practices

Paolo Falcarin*
School of Architecture, Computing and Engineering
University of East London (UEL)
Docklands Campus, E16 2RD
London, United Kingdom
falcarin@uel.ac.uk , +44 20 8223 6086
**main contact person*

Brecht Wyseur
Nagravision S.A.
Route de Genève 22-24,
1033 Cheseaux-sur-Lausanne, Switzerland
brecht.wyseur@nagra.com

***Abstract (for ICSE website)* - The need for adequate protection of software is clear. Critical infrastructures need to be protected against vulnerability exploitation; games against cheating; our banking applications against malicious tampering; or software vendors need to protect their software against piracy – to just name a few. Despite the fact that a lot of research has been conducted in the past decade in the area of Code Obfuscation and Software Anti-Tampering, software applications are often still vulnerable. That is because we need better techniques; we need to be able to evaluate the robustness thereof; and we are missing appropriate tools.**

The aim of this workshop is to bring together researchers and industrial practitioners both from software protection and the wider software engineering community to discuss software protection techniques, evaluation methodologies, and tools, in order to define directions for future research.

The workshop objective is creating a community working in this new growing area of security, and to highlight its synergies with different research fields of software engineering, such as: software modelling, program analysis, reverse engineering, code transformation, testing, empirical evaluation, and software metrics.

***Index Terms*—Obfuscation, Information Hiding, DRM, remote attestation, tamper-proofing, reverse engineering, security evaluation, empirical experiments, software diversity, renewability.**

1. Introduction and motivation

Software Protection is crucial for many individuals and companies that produce or use software; these may be software vendors, or any service industry relying on software applications. Software protection is crucial to mitigate attacks such as reverse engineering, piracy, and tampering.

Software engineers need to be aware of these threats, and companies need to organize appropriately. Secure coding is a first step. Inevitably, the development and build process need to be impacted as appropriate tools to deploy protection techniques need to be deployed. That is a challenging step for many companies. And last but not least, it needs to be ensured that the robustness achieved is adequate. All these steps are vital to defend companies' or individuals' assets such as service keys, intellectual properties, and program execution correctness. Effective deployment of protection techniques can mean the difference between business survival and failure.

A computer system's security can be compromised in many ways. A denial-of-service attack can make a server inoperable, or an eavesdropper can reap financial rewards by intercepting the communication link between a customer and her bank through a man-in-the-middle (MITM) attack.

What all MITM scenarios have in common is that the adversary is an untrusted entity that attacks a system from the outside. If we remove this assumption and if we allow anyone operating a computer system (from system administrators down to ordinary users) to compromise that system's security, we find ourselves in a more complex scenario that has received comparatively little attention. Methods for protecting against such Man-At-The-End (MATE) attacks are variously known as tamper-proofing techniques, digital asset protection, or, more commonly, software protection.

More in general, software protection research aims at developing algorithms that protect the integrity of data and software applications deployed on un-trusted devices.

2. Relevance to Software engineering

Software Protection has been an intrinsic problem of software engineering since software has become a commercial product: Fig. 1 shows the cover of the tech-news journal *The Transactor* (published in Canada), and its special issue on Software Protection and Piracy.

Commodore 64: Quadra 64 – Write 4 Programs At Once!
The Transactor
The Tech/News Journal For Commodore Computers Vol. 5
Issue 03
$2.95
NOW 95% Ad Free!
Software Protection And Piracy
• Butterfield: Comparing BASIC Programs
• Password Protection Techniques
• Lockdisk: Forces RUN on LOAD
• Scrambling A BASIC Program
• DiskMod: Recover Lost Data
• Legal Aspects of Piracy
November 1984
Plus: Nearly Every Program Protection Method We Know Of!

Fig.1: The Transactor magazine

Such issue was published in November 1984 and dedicated to Software Protection problems for the glorious Commodore-64 personal computer. This example shows how piracy is a long-standing problem, while software protection has just recently evolved from a set of disparate technical tricks into a proper research field.

Software protection is an area of growing importance in software security: leading-edge researchers have developed several pioneering approaches for preventing or resisting software piracy and tampering but only recently, one comprehensive textbook on the subject has been published [1].

Software Protection scope spans a range of different heterogeneous research topics: obfuscation and cryptography [2], digital rights management [3], information hiding [4], reverse engineering [5], compilers and code transformations [6], and distributed systems [7].

Software protection is relevant to software engineering and a challenge for software engineers, for several reasons.

First, as protections typically consists of components injected into software and of transformations applied to the original, non-protected software to invoke the protections, a good software architecture is needed to integrated multiple protections. This is a non-trivial design issue.

Secondly, software protections provide non-functional features, of which the deployment should ideally not put a burden on the designers and developers of the software to be protected. This implies that tools should deploy the protections (semi-)automatically and that non-security experts should be able to deploy the tools. This is an open challenge. For example, even the simple specification of the assets in the software to protect and of the threats to mitigate (which depend on the software but also on the business model of the vendor) is a complex problem. And so is the reporting of the provided protection to the software developer.

Thirdly, as software protections try to prevent MATE attacks, they unfortunately also prevent benign activities such as debugging and coverage analysis. How to reconcile software protections with software engineering activities such as validation, testing, debugging, and certification is an open challenge.

3. Themes and goals

This workshop will consist of a selection of articles aimed at providing software engineers with appropriate methods, approaches, techniques, and tools to support evaluation and integration of software protection techniques into their software products. The articles will present mechanisms and strategies to mitigate one or more of the problems faced by software protection.

The goal of this workshop is to bring together researchers and industrial practitioners both from software protection and the wider software engineering community to share experience and provide directions for future research, and to stimulate the use of software engineering techniques in novel aspects of software protection

The workshop aims at creating a community working in this new growing area of security, and to highlight its synergies with different research fields of software engineering, like: software modelling, program analysis, reverse engineering, code transformations, testing, empirical evaluation, and software metrics.

The target audience of this workshop will be scholars and practitioners who are interested in getting a clear state-of-the-art understanding about the possible menaces to their intellectual property, and the related advantages and disadvantages of different software protection techniques, and who wants to gain practical knowledge about how to deal with such techniques and tools in order to protect their work from existing threats.

Articles in this workshop might also investigate usage of software protection by malware, including techniques to contrast reverse engineering, and avoid anti-virus detection.

Examples of research questions are

- What are the current threats to intellectual property and what are the key protection mechanisms?
- How to evaluate and compare different protection tools and techniques?
- What lessons can be learned from failures due to the lack of attention to software protection?

- How is software protection used to prove authorship and tracking violation?
- How to evaluate the effectiveness of software protections? How long before the software will be cracked?
- How to deploy software protection with minimal interference with existing software design and development processes.

4. Organization

The desired length of the workshop is one day, possibly on Tuesday 19th. However we can accept to move it on other permitted days, with preference of Monday 18th rather than Saturdays or Sundays, as many possible participants from industry would not be able to attend in week-ends.

The basic equipment needed is a projector, a whiteboard, wifi connection, desks to accommodate people with laptops, power sockets, room capacity for 20 to 50 people;

The workshop will be open and we will solicit participation from people from different communities in software engineering to explore the synergies with software protection; in the software security domain we will advertise the workshop in the ASPIRE project website [9] and to the consortia of other related projects.

We have already established a community of people working in software protection through the former RE-TRUST workshops in 2008 and 2009, the special issue of IEEE Software in 2011, and the international summer schools on software protection [12].

The two editions of RE-TRUST workshop ran for 2 days with about 30 attendees and we expect a similar number of participants;

A draft workshop webpage [10] has been created on the website of the ASPIRE FP7 project [9], with the call for papers.

The workshop structure will start with full papers (30 min. presentations) in the morning session, possibly starting with an invited speaker. In the afternoon there will space for be short papers (15 min presentations), with particular emphasis for industrial contributions, position papers and PhD student contributions. The workshop will conclude with a panel of software protection experts.

5. Organizers and Program committee

A. Paolo Falcarin

Paolo Falcarin is a Reader (Associate Professor) at University of East London. He got his Ph.D. in Software Engineering in 2004 at Politecnico of Torino (Italy). His research interests are: software protection for distributed systems, renewable and tamper-resistant software, system modelling, service oriented computing.

Paolo Falcarin was one of the guest editors of the special issue on software protection of IEEE Software in 2011 [8].

Moreover, he organized the Telecom Service Oriented Architecture workshop (TSOA 2007), affiliated with ICSOC 2007 in Vienna (Austria): it was a one-day workshop bringing together more than 25 participants from industry and academia on service oriented computing in the telecommunications domain [12].

B. Brecht Wyseur

Brecht Wyseur is a security architect and cryptography expert at Nagravision S.A., a Kudelski Group company, world leader in digital security and convergent media solutions for the delivery of digital and interactive content.

His main interests are shared between cryptography and software security: Cryptography, computer security, security architectures (CAS and DRM), white-box cryptography, software security (obfuscation, software tamper resistance, and remote attestation).

He obtained his PhD from KULeuven, Belgium, in 2009. Prior to that, he received a master degree in mathematics from KULeuven. In the latest years, he has been active in several research projects on cryptography and software security funded by the European Commission, the Flemish and the Belgian government; published at international conferences and journals, filed patents, and have been a regular invited speaker.

In the past he organized two editions of RE-TRUST workshop in 2008 and 2009 in Italy: they were two-day workshops bringing together more than 40 participants from industry and academia on remote entrusting and software protection [8].

C. Program Committee

List of program committee members:

- Jerome d'Annoville – Gemalto, France
- Jean Daniel Assel – Gemalto, France
- Cataldo Basile - Politecnico di Torino, Italy
- Mariano Ceccato -- Fondazione Bruno Kessler, Italy
- Christian Collberg – University of Arizona, USA
- Bart Coppens - University of Ghent, Belgium
- Mila Dalla Preda – University of Verona, Italy
- Koen DeBosschere – University of Ghent, Belgium
- Bjorn DeSutter - University of Ghent, Belgium
- Werner Dondl – SafeNet Inc., USA/Germany
- Michael Franz – University of California, Irvine, USA
- Roberto Giacobazzi – University of Verona, Italy
- Johannes Kinder – Royal Holloway Univ. of London, UK

- Antonio Lioy – Politecnico di Torino, Italy
- Isabella Mastroeni - University of Verona, Italy
- Christian Mönch – Conax, Norway
- Mattia Monga – University of Milan, Italy
- Riccardo Scandariato – Chalmers University, Sweden
- Christophe Tartary – University of East London, UK
- Clark Thomborson, University of Auckland, New Zealand
- Paolo Tonella -- Fondazione Bruno Kessler, Italy
- Gaofeng Zhang – University of East London, UK
- Michael Zunke – SafeNet Inc., USA/Germany

Short list of possible committee members or contributors:

- André Nicoulin – Nagravision, Switzerland
- Mikhail Atallah – Purdue University, USA
- Ginger Myles, IBM Almaden Research Center - USA
- Alexandre Gazet -- Sogeti, ESEC, France
- Yoann Guillot -- Sogeti, ESEC, France
- Haya Shulman – University of Darmstadt, Germany
- Andy King – University of Kent, UK
- Mariusz Jakubowski - Microsoft Research, USA
- Jens Krinke - University College London, UK
- Jasvir Nagra - Google Inc., London, UK
- Yuan Gu – Irdeto, USA
- Wei-Ming Khoo, University of Cambridge, UK
- Mihai Christodorescu, Qualcomm, USA
- Prashant Gupta, McAfee Labs, UK
- Stefan Katzenbeisser - Philips Research, Netherlands
- Klaus Kursawe -- Philips Research, The Netherlands
- Bart Preneel -- Katholieke Universiteit Leuven, Belgium

Acknowledgment

The workshop is partly sponsored by the ASPIRE project [9], funded from the European Union Seventh Framework Programme FP7 under grant agreement number 609734.

References

[1] C. Collberg, J. Nagra. Surreptitious Software: Obfuscation, Watermarking, and Tamperproofing for Software Protection. Addison Wesley, 2009.

[2] Garg, S., Gentry, C., Halevi, S., Raykova, M., Sahai, A., & Waters, B. (2013, October). Candidate indistinguishability obfuscation and functional encryption for all circuits. In Foundations of Computer Science (FOCS), 2013 IEEE 54th Annual Symposium on (pp. 40-49).

[3] Zeng, Wenjun, Heather Yu, and Ching-Yung Lin, eds. Multimedia security technologies for digital rights management. Vol. 18. Academic Press, 2011.

[4] Brecht Wyseur, "White-box cryptography: hiding keys in software." NAGRA Kudelski Group (2012).

[5] Dube, T.E. Birrer, B.D. Raines, R.A. Baldwin, R.O. Mullins, B.E. Bennington, R.W. Reuter, C.E.: Hindering Reverse Engineering: Thinking Outside the Box, IEEE Security & Privacy, 2008, Vol 6(2), pp 58-65

[6] S. Debray, W. Evans, R. Muth and B. De Sutter, Compiler Techniques for Code Compaction. In ACM Transactions on Programming Languages and Systems, 22(2), March 2000, pp. 378-415.

[7] R. Scandariato, Y. Ofek, P. Falcarin, and M. Baldi, "Application-Oriented Trust in Distributed Computing," in Proceedings of the 2008 Third International Conference on Availability, Reliability and Security. IEEE Computer Society, 2008, pp. 434–439.

[8] P. Falcarin, C. Collberg, M. Atallah, and M. Jakubowski. "Guest Editors' Introduction: Software Protection." Software, IEEE 28, no. 2 (2011): 24-27.

[9] EU FP7 ASPIRE project (Advanced Software Protection: Integration, Research and Exploitation). On-line at http://www.aspire-fp7.eu/

[10] International Workshop on Software Protection (draft homepage). On-line at http://www.aspire-fp7.eu/spw2015/

[11] RE-TRUST workshops. On-line at http://re-trust.dit.unitn.it/

[12] International Summer School on Information Security and Protection, 2011, 2012, 2013 and 2014 editions online On-line at http://issisp.elis.ugent.be/, http://profs.sci.univr.it/isisp12/ISISP12/Welcome.html, http://issisp2013.nwu.edu.cn/, and http://issisp2014.di.univr.it/.

[13] Telecom Service Oriented Architecture Workshop, 2007. On-line at http://icsoc2007.servtech.info/workshops.html