SIAM

SECURITY IMPACT ASSESSMENT MEASURES

Metro-Station Torino

Research consortium meeting in Torino (Italy)

The consortium had its biannual meeting between September 10th – 12th in Torino, at Istituto Superiore sui Sistemi Territoriali per l'Innovazione (SITI).

Beside the presentation of the final results of work package 2, 5 and 7, the consortium discussed the methodological guidelines for the upcoming work packages 8 and 9. TUB presented the theoretical approach of the assessment model. After an intensive discussion, the consortium decided that SIAM framework will be based upon three hierarchic levels that should allow for cross-links, overlaps and a more complex interrelation between the objects, attributes and attributes of attributes:

- The basic level is represented by four basis **CONCEPT FAMILIES:** Security, Trust, Efficiency and Freedom Infringements.
- Descending from Concept Families, are **ASSESSMENT CRITERIA** (for example Transparency, or Liability), that represent the middle level of evaluation. A single Assessment Criteria can be linked to more Concept Families.
- Descending from Assessment Criteria, are **ATTRIBUTES** (for example infringement of the right to data protection or infringement of the right to non-discrimination), that represent the lower level of evaluation. Each attribute is associated with a specific question, which will be part of the SIAM Assessment Support process. A single attribute (and associated question) can be linked to more Assessment Criteria.

Furthermore, the consortium agreed on a common action plan until the end of the project. During the meeting the whole SIAM consortium was invited by Metropolitana di Torino to introduce the consortium to the security concept of a public transport system. A guided tour through the premises was also organized by the Metropolitana di Torino.

In this issue

- Meeting Torino
- Support System Tool
- Announcements
- Activities
- Work packages

Partners

Kingston University London

The Assessment Support System Tool

SIAM Assessment System Wireframe

Task leader:
Kingston University London (UK)

In the recent months, an interactive wireframe of the future SIAM Assessment Support System has been developed (Figure 1). The purpose of creating this software mock-up was to demonstrate possible SIAM functionalities to end users, test user interaction with the proposed design, and collect feedback from the users.

The system is based on the specification described in deliverable D11.1 and illustrates a good part of the functionality related to the three functional units of the SIAM ASS: Assessment Configuration, Information Gathering and Advice, and Report Generation. A particular challenge in designing this system was to provide all the input- and display-facilities for the many kinds of information that are being handled by SIAM, whilst managing the space that is available for the entire application on screen.

In its latest state of development, the wireframe provides a highly interactive user experience. Users are able to progress through the entire idealised technology acquisition process, starting from defining and editing an assessment context, answering sets of assessment questions, and generating an example report. A wide range of auxiliary functionality (e.g., login screen, opening and saving of files, managing the user account, etc.) can be demonstrated as well.

The SIAM ASS wireframe was presented to actual end users at the user forum at TUB in Berlin on 13 December 2012. Visitors in-
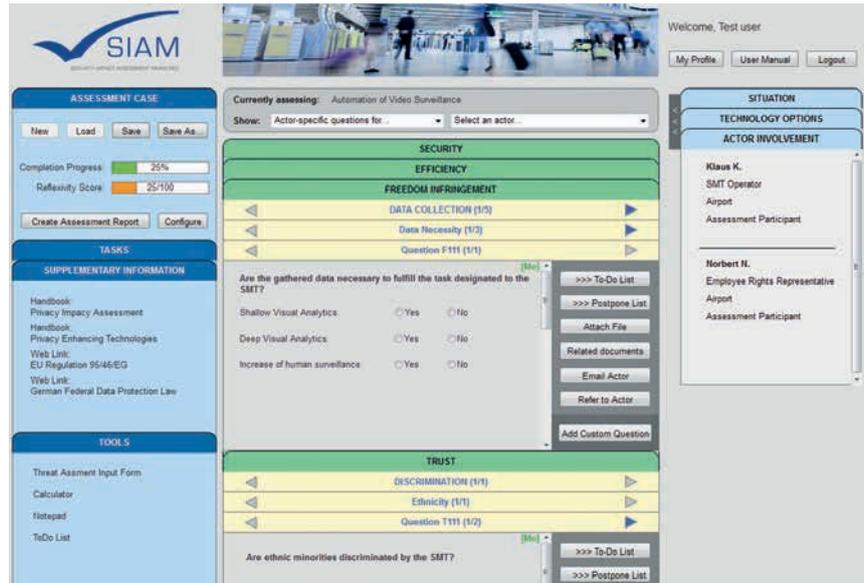

Figure 1: A screenshot of the SIAM ASS wireframe, version 4.
http://staffnet.kingston.ac.uk/siam/userforum1/SIAMASS4/Login.html

cluded managers from the Berlin Airport and researchers in the respective fields. A practical example involving an airport security incident was used to introduce the participants to the features of the system and demonstrate how to interact with its graphical interface. After that, everyone was free to test the system by themselves. Each participant was accompanied by an assistant who to respond to any questions and collect feedback from the user.

The feedback given by the participants of the forum was very positive throughout. Further

user forums will be held in Torino (Italy), Tel Aviv (Israel) and in Berlin once again. Together with the results of a range of upcoming activities (e.g., development meetings, validation workshops), insights gained will be used to inform the development of the SIAM ASS over the course of the next 3 months. It is planned to finalise the requirements analysis for the system specification by May 2013, after which the development of the first version of the prototype will go ahead.

SIAM is subdivided into 13 Work packages

WP 1 - Project: Management
WP 2 - Security technology innovation journeys
WP 3 - Impact analysis on criminal actions liegt;
WP4 - Regime interaction and freedom infringements
WP 5 - Future technologies
WP 6 - Threat scenarios
WP 7 - Criminal actions – patterns & places
WP 8 - Freedom scenarios
WP 9 - Legal frameworks – Regulative Techniques
WP 10 - Cultural differences
WP 11 - The SIAM database
WP 12 - The Security Impact Assessment Measure
WP 13 - Dissemination

Duration: February 2011 – February 2014

Work package No. 3

"Impact analysis on criminal actions"

WP Leader: Technische Universität Berlin (D)
Duration: 09/2012 – 09/2013

In September 2012 work began on work package 3. The overall objective of work package 3 is to capture frequent and dangerous criminal offenses at airports and in public transport systems and of proper ways to deal with them. Based on the methodology developed in work package 7 "Criminal actions-patterns & places" the SIAM consortium will

conduct a series of workshops to analyse how the impact of SMTs on criminal actions is being assessed. Understandings of frequent and dangerous crimes, proper ways to deal with them and unintended consequences of SMTs will be fed into the SIAM database as assessment criteria, attributes and questions.

Work Package No. 8

Freedom Scenarios

WP Leader: Vrije Universiteit Brussels (B)
Duration: 09/2012 – 03/2013

The main focus of WP8 is to develop freedom scenarios. These are narratives that will depict the types of freedom infringements that may be possible in relation to different kinds of SMTs, and they will illustrate how these infringements could unfold along the four freedom infringement dimensions and how they might be mitigated. To that end WP8 will draw on the findings from WP2 and WP4 in which an SMT-typology (WP2, D.2.3) and an infringement typology (WP4, D.4.2) was developed.

In WP8 we will first amend and refine the combined findings from WP2 and WP4 by conducting expert interviews which will further clarify which infringement problems the different SMT types pose. These findings will provide an input for a workshop that will be conducted by each of the SIAM partners. In the workshops experts will evaluate 4 SMTs, one from each category of the SMT-typology, and the infringement problems they pose.

These evaluations will be done on the basis of the infringement typology. The expert evaluations will provide the basis for the 4 "worst-case" scenarios that each partner will develop for the final scenario report. For those same SMTs, experts will also evaluate how these infringement problems might be mitigated. These evaluations will result in findings that will be used to develop 4 "best-case" scenarios for the final scenario report.

As such, the objective of each of the workshops is to provide the empirical basis for the development of 8 scenarios, 4 worst-case and 4 best-case scenarios, that will clarify the complex nature of the freedom infringements that come with the deployment of particular SMTs and they will show how such infringements might be mitigated.

WP8 will result in a freedom scenario report in which all the scenario narratives are analyzed and documented so that generic conclusions can be drawn (D.8.1). The data will be structured for integration in the database and will furthermore be used to develop assessment criteria and questions for the SIAM tool (D.8.2).

Work Package No. 8

'Legal Frameworks – Regulative Techniques'

WP Leader: Universität Kassel (D)
Duration: 09/2012 – 09/2013

Work on WP9 began in September 2012. Its general purpose is to gain an understanding of the legal framework that regulates the use of SMTs and to find out whether implemented regulative techniques actually achieve their objectives and whether they are ready to face the challenges of evolving, more intensive and extensive SMTs. To achieve this, WP9 will build on the information gathered in all previous work packages. However, WP9 is most closely connected and related to WP2, WP4, WP5 and WP8. WP2 and WP5 have provided information on present and future technologies and will give an indication for the challenges that the legal regulation of SMTs poses. WP4 has looked at different groups of actors that come in contact with SMTs. WP8 will amend this by providing insight into the types of freedom infringe-

ments passengers are subjected to when using mass transportation systems. All in all, together with WP8, WP9 is aimed at adding a distinct legal perspective to the work that has already been conducted over the course of the project.

WP9 will produce four case study reports together with an evaluation. The main input to the SIAM Assessment Support System will however be a method for the legal evaluation of security measures based on the KORA method (German: Konkretisierung rechtlicher Anforderungen; Concretization of Legal Requirements) which has been created at the Project Group Constitutionally Compatible Technology Design to assist the development process of information technologies. This will be amended by VUB who will work with KORA to develop what they call 'legal protection by design'. VUB will also look at the regulatory framework of the use of SMTs at EU and international level.

Work Package No. 10

'Cultural differences'

Work package leader: SiTi (I)
Duration 03/2013 – 09/2013

Its general purpose is to reveal national cultural differences in the attitudes towards different types of SMTs that lead to different levels of acceptance.

Apart from institutional standards, every member states' people have their own individual attitudes towards security technologies and a distinct level of freedom infringement that individuals and societies are willing to accept. The necessary trade-offs between security measures and some level of freedom infringement, e.g. affecting one's physical privacy during airport control, will be balanced quite differently for cultures or social groups within cultures. Both security and freedoms are perceived in conditional ways, and technology within the context of security might not take on the same meaning for all actors.

To achieve this, WP10 will build on the information gathered in all previous work packages, in particular WP 4 and WP 8 which will help on defining the interrelations between freedom infringements and people attitudes with reference to different security technologies typologies. While some feel that physical intrusiveness is the strongest form of infringement, others will be much more aware of their data being dispersed globally – depending on cultural practices and technological developments. Last but not least, the infringements might not be perceived equally for all groups. Gender, age, and status are important categories to be included in the analysis. Thus, the infringement dimensions can be used to create another mapping for cultural differences.

A second resource for the analysis of attitudes towards anticipated future security technologies is media coverage. Freedom infringements as well as security benefits from security technologies are discussed in print media, online, and on TV. Media analysis will provide a rough overview of quantitative levels of coverage, and in-depth analysis of the attitudes expressed. Scandals, technology renaming ("body scanner") and lawsuits obviously point to strong attitudes against a measure.

A third resource will come from interviews with engaged stakeholders (such as civil rights representatives interviewed in WP8) which will be asked for their attitude towards a number of selected foreseeable SMTs.

Activities

Computer, Privacy & Data Protection Conference

SIAM supports Data Protection Account-ability – Panel on CPDP Conference

Wednesday, January 23, 15:30,
Data Protection Accountability – Who cre-ates the account?

Impact Assessments are a way to foster Data Protection Accountability as supposed by the Article 29 Working Parties Opinion 3/2010 "On the principle of accountability".
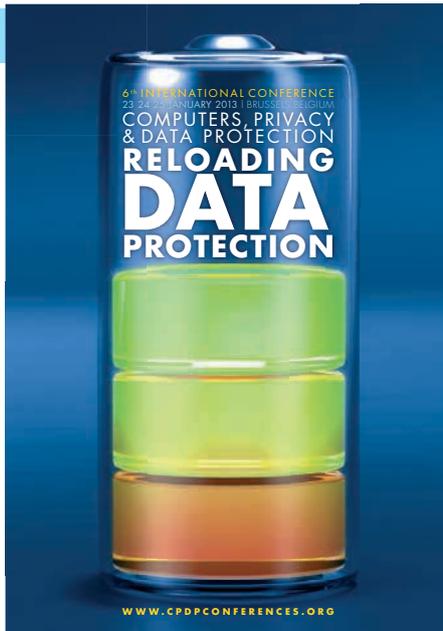
The SIAM tool will provide possibilities to ren-der accountability in the decision processes and thus support compliance with upcoming regulations. SIAM is co-organizing a panel of the Computers Privacy and Data Protection Conference to discuss different approaches to implement accountability. Brendan van Alsenoy

(KU Leuven, BE), Denis Butin (INRIA, FR), To-bias Bräutigam (Nokia, FI) and Peter Schaar (Federal Commissioner for Data Protection and Information Germany) will give different perspectives on how to "create the account".

More details on
www.cpdpconferences.org

Announcements

Technical University Berlin hosted two workshops.

The first workshop took place on the 2nd of February. The participants were experts from various fields of airport security (policy, enforcement, management). The scenario based workshop tested the STEP model and validated the empirical data gathered in work package 2.

The second workshop was co-organized by University of Kassel and Technical University Berlin and was held on the 16th of April in Berlin. The workshop focused on assess-ment of the developed threat scenario methodology in Work Package 6. The law enforcement experts discussed two key threats for airport security; illegal migration and organized crime.

It is a great opportunity to meet academ-ics, policy makers and practitioners in this field of competence and to exchange best practice for the further development of the SIAM methodology.

More: http://pacita.strast.cz/en/conference/general-info

February 27th, 2013 in Berlin (Germany)

Workshop: Assessment criteria interrela-tions and interdependencies

The research consortium will meet in Berlin to validate the developed assessment crite-ria with their respective attributes. A special focus will be set on the interdependencies and –relations between them.

March 13th – 15th, 2013
in Prague (Czech Republic)

Technology Assessment and Policy Areas of Great Transitions Conference

SIAM got accepted to be presented in context of the first Technology Assessment Conference in Prague in March this year.

Contact

Project coordinator:
Dr. Leon Hempel
Centre for Technology and Society
Technische Universität Berlin
Phone: +49/30/314 25373
Email: hempel@ztg.tu-berlin.de

Dissemination:
BBAA e.V.
Email: info@siam-project.eu

Internet: www.siam-project.eu
Production: www.layoutmanufaktur.de