3.1 TREsPASS Publishable summary

Project overview

Information security threats to organisations have changed completely over the last decade, due to the complexity and dynamic nature of infrastructures and attacks. Successful attacks cost society billions a year, impacting vital services and the economy. Examples include StuxNet, using infected USB sticks to sabotage nuclear plants, and the DigiNotar attack, using fake digital certificates to spy on website traffic. New attacks cleverly exploit multiple organisational vulnerabilities, involving physical security and human behaviour. Defenders need to make rapid decisions regarding which attacks to block, as both infrastructure and attacker knowledge change rapidly.

Current risk management methods provide descriptive tools for assessing threats by systematic brainstorming. Attack opportunities will be identified and prevented only if people can envisage them. In today's dynamic attack landscape, this process is too slow and exceeds the limits of human imaginative capability. Emerging security risks demand tool support to predict, prioritise, and prevent complex attacks systematically.

The TREsPASS project will develop methods and tools to analyse and visualise information security risks in dynamic organisations, as well as possible countermeasures. An "attack navigator" will be built to identify which attack opportunities are possible and most pressing, and which countermeasures are most effective. To this end, the project combines knowledge from technical sciences (how vulnerable protocols and software are), social sciences (how likely people are to succumb to social engineering), and state-of-the-art industry processes and tools, such as The Open Group's ArchiMate.

By integrating European expertise on socio-technical security into a widely applicable and standardised framework, TREsPASS will reduce security incidents in Europe, and enable organisations and their customers to make informed decisions about security investments. This increased resilience of European businesses both large and small is vital to safeguarding the social and economic prospects of Europe.

The TREsPASS consortium comprises the entire value chain, including academic researchers in the social and the technical sciences, researchers and practitioners from large multinational companies, and developers and practitioners from SMEs. TREsPASS is coordinated by Prof. Pieter Hartel of the University of Twente. The other partners in the project are the Technical University of Denmark, Cybernetica (Estonia), GMV Spain, GMV Portugal, Royal Holloway University of London (United Kingdom), itrust Consulting (Luxembourg), Goethe University Frankfurt (Germany), IBM Research – Zurich (Switzerland), Delft University of Technology (Netherlands), Hamburg University of Technology (Germany), the University of Luxembourg (Luxembourg), Aalborg University (Denmark), Consult Hyperion (UK), BizzDesign (Netherlands), Deloitte (Netherlands), and Lust (Netherlands).

The project consists of the following work packages:

LIST OF WORK PACKAGES (WP)						
WP Number [53]	WP Title	Type of activity [54]	Lead beneficiary number [55]	Person-months [56]	Start month [57]	End month [58]
WP 1	Socio-technical security model specification	RTD	2	168.00	1	48
WP 2	Data management process	RTD	4	208.00	1	48
WP 3	Quantitative analysis tools	RTD	1	178.00	1	48
WP 4	Visualisation process and tools	RTD	6	89.00	1	48
WP 5	Process integration	RTD	3	132.00	1	48
WP 6	Tools integration	RTD	7	86.00	1	48
WP 7	Validation through case studies	RTD	8	137.00	1	48
WP 8	Project Management	MGT	1	48.00	1	48
WP 9	Standardisation, Dissemination, and Exploitation	OTHER	9	76.00	1	48
			Total	1,122.00		

Table 1: List of Work Packages (WP)

Results to date

At the 6 month milestone (MS3), initial requirements have been defined for all work packages, based on overviews of the state-of-the-art. The initial requirements have been laid down in Deliverables DX.1.1. At the 12 month milestone (MS4), prototypes have been developed for (a) model, (b) data extraction and for (c) the tools. Reports on the analysis methods and on the abstraction levels for model sharing were elaborated. Finally, the plans for dissemination/exploitation and standardisation were prepared and reports now document the results achieved so far.

A number of fundamental choices have been made to assure alignment between the work packages:

- Attack trees as the initial unit of data exchange between the work packages, with the intention to lift this assumption after the first year;
- A clear separation between the system model (navigator map) and the attacker model;
- Risk concepts and process workflow based on the Risk Taxonomy of The Open Group (FAIR);
- A loose coupling of modules with a central integration component, data exchange by means of XML;
- Internet Protocol Television (IPTV) payment as a concrete case for the customer privacy protection case study, and two fraud cases for the telecommunications case study.

In Year 1 the TREsPASS consortium has already achieved several significant results relevant for the project, as well as scientific innovations that advance the state-of-the-art.

Key project results

1. **Grounding of project work in state-of-the-art and practical requirements.**
   - We have **performed systematic reviews** (*e.g*. on attack trees (completed) and system models (on-going)) and **interview studies** (*e.g.* auditor interviews) to root the project work on the state-of-the-art, and identify important techniques to add to the TREsPASS tools.
2. **First prototype of the TREsPASS tools.**
   - We have **realised the first integrated prototype of the TREsPASS tools** using XML-based exchange formats.
   - We have developed
     - **Systematic methods for generating attack trees** from system models. This is the first step towards explicit navigator maps and attacker profiles.
     - **Efficient analysis of attack trees**, our internal representation of attacks.
     - **Context-dependent risk visualisations** with measurable expressivity to communicate models and analysis results to end-users.
   - We have **extended attack trees with libraries** that represent common patterns for realising attacks. These libraries contribute parts of attack trees that would require modelling of non-relevant details. This contributes to better understandable models.
   - We have **established the first link to project-external approaches** to risk assessment. By linking the TREsPASS tools to ArchiMate and the Open Group Risk Taxonomy (FAIR), we are able to interface to the outside world for assessing relevance.
   - A **significant part of a real-world SME case study has been modelled**, analysed, and visualised using the TREsPASS tools and methods, and has been presented to the case-study owner, who was excited about the results.
3. We have **started dissemination and standardization** activities, including:
   - We have established a category C **liaison with ISO/IEC JTC 1/SC 27/WG 1 and WG 4,** and have started contributing to The Open Group ArchiMate and TOGAF industry standards;
   - We are **contributing to the Network and Information Security Public-Private Platform (NIS PPP),** with representatives in all three working groups;
   - We are **co-organising the International Workshop on Graphical Models for Security** (GraMSec 2014); and
   - We have submitted a **successful proposal for a Dagstuhl seminar** on Socio-technical security metrics, to take place November 30 – December 5, 2014.
   - We have presented TREsPASS results at many scientific conferences.

Scientific innovations

1. A new method has been proposed to overcome one of the major limitations of attack trees, by including Bayesian reasoning. These so-called **Bayesian attack-defence trees** extend attack-defence trees with dependencies. Several further extensions are under development.
2. A **separation of attacker profiles and system models** has been developed to enable adaptations of risk analysis upon changes in the threat environment. This method also allows us to select standard attacker profiles and infrastructure components from libraries.

3. A new method has been proposed for enabling the inclusion of penetration testing results in risk management. **Quantitative penetration testing** does not only measure whether certain attacks are possible, but also how easy or difficult they are. The skill of the penetration testers is assessed as well, and this is included in the estimations.
4. A novel method of **baselining visual expressivity** has been prototyped and initially evaluated in terms of comparing the communication of narrative content between different user groups. The method of baselining expressivity (based on McCloud's method of evaluating the expressivity of comics) will be adapted for a range of expressivities where the types of expressivity to be evaluated will be derived from the results of TREsPASS fieldwork.
5. We have developed a method to **systematically generate attack scenarios** from navigator maps, by exploring the paths through which an attacker can invalidate a security goal. Quantitative properties in the maps are transferred to the scenarios, and can be used in risk analysis.

Both the core project results and the scientific innovations contribute to the integration of theory and practice around graphical security models in Europe, and to the further development of more mature cyber security risk management tools and processes in the upcoming years of the project.

Expected final results

The TREsPASS project will provide the following innovative results:

1. The overall TREsPASS framework that organisations can employ to embed the analytic, model-based methods in their risk management processes, consisting of:
    - A process for the iterative development of **socio-technical security models** (navigator maps plus attacker models);
    - Tools for **prediction** of attacks and associated properties from socio-technical security models;
    - Tools for **prioritisation** of the attacks according to these properties;
    - Tools for **prevention** by calculating the effects of countermeasures, and ranking the countermeasures according to their cost-effectiveness;
2. A demonstrator tool to integrate the above analyses;
3. Validation of the overall process by means of three case studies;
4. New and/or refined organisational and behavioural theories based on the data acquired in the process of model building.

Project website

www.trespass-project.eu