TRE$_S$PASS Y4 publishable summary

Key takeaways

- The TRESPASS project has reached its M48 milestone, with deliverables on sociotechnical security models and specification languages, data extraction tools, information system, information testing and degradation tools, attack generation, dynamics of stochastic models, visualization methods, model maintenance, processes, deployment and maintenance plan, tool integration and case studies,
- TRESPASS developed the Attack Navigator and has validated the methods and tools in 5 case studies and,
- In Year 4 TRESPASS produced a total of 2 journal publications with an ISI impact rating, 1 invited book chapter, 21 peer-reviewed publications at international conferences attended by over 1270 scientists and many interactive dissemination events demonstrating the relevance of project outcomes and further increasing impact potential. Furthermore, the project has organised 4 academic events.

Project overview

Information security threats to organisations have changed immensely over the last decade, due to the complexity and dynamic nature of infrastructure 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 TRE$_S$PASS project developed methods and tools to analyse and visualise information security risks in dynamic organisations, as well as possible countermeasures. An Attack

Navigator was built to identify which attack opportunities are possible and most pressing, and which countermeasures are most effective. To this end, the project combined 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, TRE$_S$PASS results 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 TRE$_S$PASS 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. TRE$_S$PASS 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 - Zürich (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).

Project Number	318003	**Project Acronym**	TRE$_S$PASS

WP No.	**WP Title**	**Type of activity**
WP1	Socio-technical security model specification	RTD
WP2	Data management process	RTD
WP3	Quantitative analysis tools	RTD
WP4	Visualisation process and tools	RTD
WP5	Process integration	RTD
WP6	Tools integration	RTD
WP7	Validation through case studies	RTD
WP8	Project management	MGT
WP9	Standardisation, dissemination and exploitation	OTHER

Table 0.1: List of Work Packages (WP)

Results of Year 4

WP1 has created the final version of the TRE$_S$PASS socio-technical security model, which is the central structure for representing socio-technical systems. The model provides the necessary abstractions for representing systems and making them accessible for the TRE$_S$PASS tools and the TRE$_S$PASS process. Based on the developments in the first 3 years of the project, WP1 has consolidated the model, and has contributed to its validation in a vast number of case studies and experiments.

WP2 has created a programmable knowledge base with well defined interfaces that solves the complex problem of providing context sensitive metrics to the TRE$_S$PASS model and to the decoration of attack trees generated from this model. The concept provides a powerful way for practitioners to combine and capture subject matter expertise with social and technical data in a specific context. This knowledge can be used by practitioners to either differentiate a service offering, or collectively combine knowledge with other practitioners by sharing knowledge bases. WP2 has formalised the various data formats and data management through a typical TRE$_S$PASS process flow. WP2 has also extended the data collection capabilities of a number of tools both for capturing Stage zero contextual information and for extracting data from technical environments. Finally WP2 has analysed the impact of data degradation on the TRE$_S$PASS approach.

WP3 has greatly extended the scope of the security analysis methods in two directions: First, the scope has been extended, from computing likelihood, cost and feasibility of attack scenarios, towards computing the effectiveness of preventive measures, and ranking them for decision support. The other direction takes into account the dynamics from real-life risk assessment in the analysis tools. In particular, we demonstrated model transformation to glue different analysis types together, and to propagate changes from the socio-technical model through all attack models for analysis, and to propagate the analysis results back to the socio-technical model. We also developed a view on the effect of data updates.

WP4 has developed a family of visualisation tools that enable different ways of picturing cyber security risk. In particular, we have developed a visualisation dashboard that enables security analysts to present complex attack trees in radial form, linear form and in non-linear form as well as methods to visualise changes to cloud environments over time. Interaction techniques such as zooming in and zooming out and stacking have been deployed so that viewers can interact with these visualisations to examine the detail. We have also designed a physical modelling process that supports brainstorming of risk scenarios and an app to convert the outputs of the brainstorming process into input for the TRE$_S$PASS models.

WP5 has successfully completed the development of the integrated TRE$_S$PASS process. The process has co-evolved with the TRE$_S$PASS toolkit and it has been applied to a diverse selection of case studies. As supporting processes, the TRE$_S$PASS service model, support for traceability, dynamic environment update and model maintenance have been developed. WP5 has also matched the TRE$_S$PASS process with other existing risk assessment frameworks, yielding to considerable advancements in the current state of the art.

WP6 Based on the prototype specification, WP6 created a management guide of the platform, an integration guide for new tools including a deployment guide and a maintenance guide. Security and functional tests have been performed. WP6 has performed a set of tests to check the correct functioning of tools uploaded on the TRE$_S$PASS platform and the input/output interfaces. These tests complemented the testing of the different tools used for field trials in WP7. Moreover, the Attack Navigator has been improved. This interface sets up an environment where all tools developed within the project and hosted on the TRE$_S$PASS platform can be viewed, accessed and connected.

WP7 has validated the TRE$_S$PASS approaches and processes by applying the TRE$_S$PASS tools to the interdisciplinary case studies. The Cloud case study used a set of tools to validate different aspects of the TRE$_S$PASS processes. Using the Telecommunication Services case study, value-based and architecture-based risk analysis approaches were validated based on the case study requirements. Under the Customer Privacy Protection case study, both the ATM and EpStan case studies were used to validate the application of geometrical data to the TRE$_S$PASS processes.

WP8 has managed the project and in the last year organized 2 successful project meetings. WP8 also organized an Advisory Board meeting which resulted in very valuable feedback, for example that due to the research nature of the project, the emphasis should be on the value added of the tools for the individual case studies.

WP9 has disseminated the project in a number of ways. Apart from presenting papers at conferences and disseminating the project at industrial events, the project organized a summer and a winter school, a Dagstuhl seminar and a TRE$_S$PASS workshop as part of the ARES2016 conference. With regards to exploitation, the relevant target customers for each tool category were identified and we provided tool details such as IPR and location. In addition, TRE$_S$PASS made a series of contributions to ISO standards, actively engaged in NIS PPP and contributed to Open Group events.

Project website

www.TREsPASS-project.eu