TRESPASS Y3 publishable summary

Key takeaways

- The TRESPASS project has reached its M36 milestone, with deliverables on socio-technical security policies, models, processes, management, extraction, sharing, analysis, visualization, prototyping, and case studies, as well as the final deliverables on integrated requirements.
- TRESPASS has further developed the Attack Navigator, which is the project's main innovation, by developing a range of automated methods that drive data into the navigator maps, by integrating a range of complementary analysis and visualisation methods, by adapting requirements to a streamlined architectural concept, and by developing two complete and complementary tool chains that demonstrate the attack navigator's applicability.
- TRESPASS has produced a total of 18 publications in journals (of which 50% have an ISI impact rating), 45 peer-reviewed publications at international conferences attended by over 2000 scientists, 2 peer reviewed book chapters, and many interactive dissemination events demonstrating the relevance of project outcomes and further increasing impact potential. Furthermore, the project has (co)organised 3 prestigious 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 is developing methods and tools to analyse and visualise information security risks in dynamic organisations, as well as possible countermeasures. An Attack Navigator is being 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, 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 3

WP1 has developed a novel approach to separate the 'who' (credentials) and the 'what' (enabled actions) in attack navigator maps, enabling improved route detection in the attack navigator. WP1 has laid the basis for modelling emerging threats by adding support for dynamic features in navigator maps and the tools working on them.

WP2 has evolved tools and techniques for data extraction from rich socio-technical environments into navigator maps, and brought them to new levels of usability. Automated methods and tools have been developed that are capable of extracting large amounts of rich data directly from cloud infrastructures into the navigator maps.

WP3 has integrated the modelling and analysis tool chain based on a streamlined architectural concept. It supports the automatic generation of attack trees from the navigator map; automated transformation of the attack trees to the input of various stochastic analysis tools; and the application of stochastic model checking algorithms to produce the analysis results. The chain has been demonstrated on a common cloud case study.

WP4 has developed a process prototype that takes analogue, physical maps into navigator maps by abstracting salient social dimensions into simple metrics. These metrics can then be used in the WP2 data and the WP3 analysis tools. WP4 has further contributed to the development of the attack navigator map by providing visual techniques used in the early prototypes.

WP5 has completed both the practitioner and attacker interviews and designed the final process requirements based on these real world inputs. Frameworks for attack pattern library and attacker profile library have been developed and the first version of the complete TRE$_S$PASS process has been designed.

WP6 led the project-wide requirements taskforce leading to final requirements and the final architecture diagram, and produced a prototype of the user interface for the integrated TRE$_S$PASS tools.

WP7 has successfully extracted data from the cloud and ATM case studies using TRE$_S$-PASS tools, for example by extracting several layers of data, including social data from a national population census (2011) database, and environmental data from other public sources to feed the ATM case study data model. WP7 has also continued to work closely with industry partners on non-standard but very relevant risks, such as roaming fraud in the telco case.

WP8 has managed the project, organised 2 successful project meetings, and amended the Description of Work to reflect important changes, including a WP2/WP9 leadership swap. WP8 also organized an Advisory Board meeting which resulted in very valuable feedback, for example that the project should validate the results of the TRE$_S$PASS process by investigating feedback loops.

WP9 has achieved deep involvement of case study partners, with frequent direct contact with relevant industrial sectors. Prominent industrial and academic events this year have included the Social Engineering Award, the Dagstuhl seminar on socio-technical

security metrics, the New Security Paradigms Workshop, and workshops on visualisation techniques, clustering, and sharing security risk visualisations for SMEs. In addition, exploitation activities began to involve third-party practitioners from different institutions (public and private) to disseminate and benchmark the TRESPASS results and to guide future developments of the project, especially under the scope of the case studies.

Strategic development of the project for Year 4

WP1 will finalise the TRESPASS formalisation of the attack navigator map, and will perform final evaluations on the case studies from WP7. Applying the Year 3 results, it will explore upcoming threats, focusing on systems with large quantities of nodes or accidental insiders, and investigate how to capture them in navigator maps, for example through model extensions.

WP2 will focus on providing the attack step metrics to the TRESPASS analytics tools in the formats that the tools require. This will mean merging technical data, social data, and external vulnerability data into a parametrised metrics Oracle. This Oracle will provide the model augmentation tools with the necessary interfaces to query metrics.

WP3 will work on attack generation, preventive measures and ranking, by refining the metrics and applying algorithms for solving two player games. WP3 will also develop support for the evolution of the models, by applying model transformation techniques to automatically propagate the changes, and feed analysis results back to the socio-technical model. Finally, tool integration will continue, especially with the visualisation tools of WP4.

WP4 will extend qualitative visualisation into a quantification of the visualisation that can be fed into the model by further developing the techniques for abstracting numerical values from the rich pictures. It will also continue to enhance the visual techniques used in the attack navigator map and by the WP3 analysis tools.

WP5 will develop the techniques necessary to maintain and share attack pattern libraries and attacker profiles that TRESPASS toolset users will need to run the TRESPASS process efficiently.

WP6 will finalise the overall tool integration and document one of the main project outputs, the integrated TRESPASS tools.

WP7 will evaluate the latest versions of TRESPASS tools in close collaboration with the case study stakeholders, including a major telecommunications company, a cloud provider, gas stations, banks and a major ATM Interbank Network provider. The objective and success criteria of this evaluation will be the possibility to introduce the innovations from the project into real world scenarios from these institutions.

WP8 will continue to manage the project.

WP9 will organise a large number of activities, including industry workshops on advanced data collection and advanced visualisation, a social engineering analysis award on risk estimation (CPDP 2016), and summer schools/winter schools on social foundations and

technical foundations, as well as preparing a Dagstuhl seminar on Assessing ICT Security Risks in Socio-Technical Systems. WP9 will prepare detailed plans for exploiting the TRESPASS tools with external partners relevant to the case studies, such as telcos, cloud providers and financial services organisations.

Expected final results

Following the Description of Work, 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 profiles);
   - 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