predict
prioritise
prevent

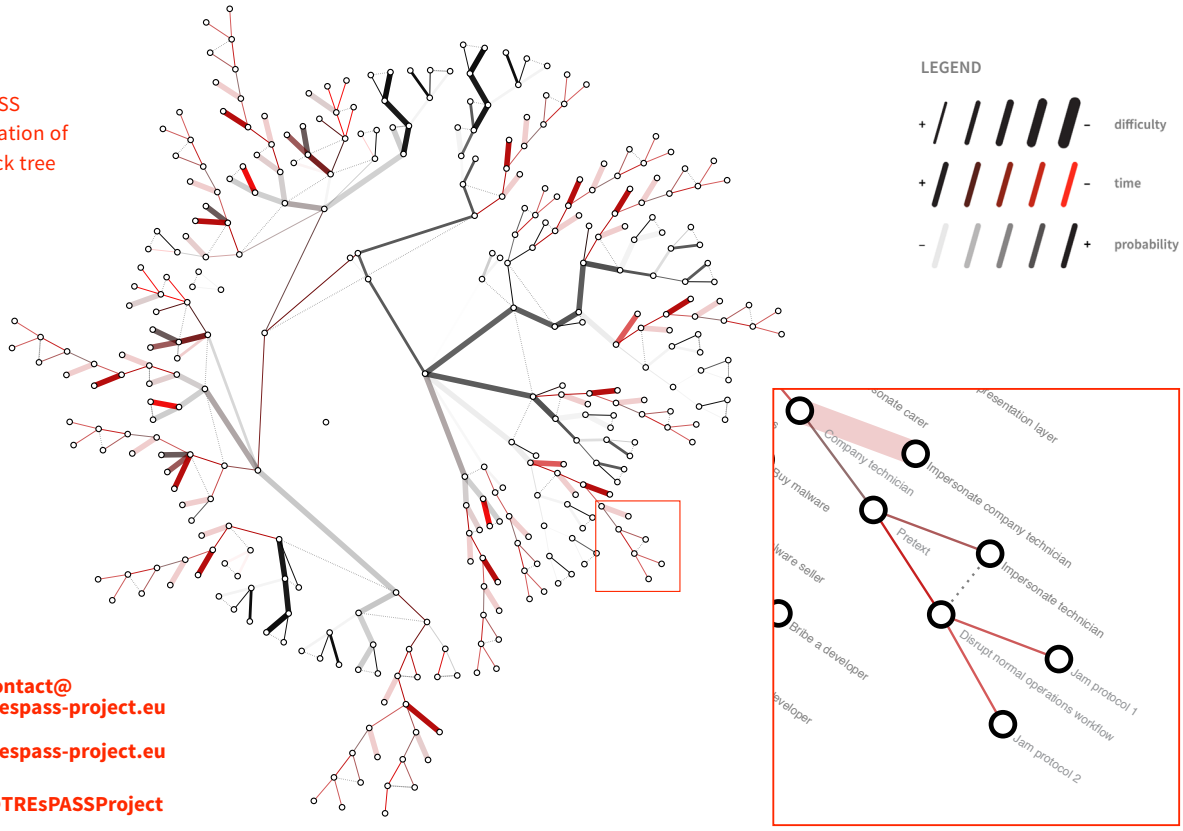
TREsPASS

Technology-Supported Risk Estimation by Predictive Assessment of Socio-Technical Security

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 (infected USB sticks to sabotage nuclear plants) and DigiNotar (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.

TREsPASS visualisation of an attack tree



contact@trespass-project.eu

trespass-project.eu

@TREsPASSProject

linkedin.com/company/trespass-project

The TREsPASS project develops methods and tools to analyse and visualise information security risks in dynamic organisations, as well as possible countermeasures. We build "attack navigators" 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 into a widely applicable and standardised framework.

The key project achievements so far are:

- Methods to systematically generate attack scenarios and associated risk metrics from navigator maps, by exploring the paths by which an attacker can invalidate a security goal.
- New extraction methods for social engineering and victimisation data to include social science data in the attack navigator risk analyses.
- A separation of attacker profiles and system models to enable selection of "plug-and-play" attacker profiles, system components and attack patterns from libraries.
- Context-dependent risk visualisations with measurable expressivity, physical (Lego) as well as digital, to discuss models and analysis results with end-users.
- Linking the TREsPASS tools to ArchiMate and the Open Group Risk Taxonomy (FAIR), as well as three different case studies, to interface to the outside world for assessing relevance.

By replacing human risk judgement with analytic identification and evaluation of attacks, TREsPASS enables better preparedness of organisations in a cyber risk society.

This project receives funding from the European Commission's Seventh Framework Programme under Grant Agreement No. 318003 (TREsPASS).