TRESPASS Y2 publishable summary

Key takeaways

- The TRESPASS project has reached its mid-project milestone, with deliverables on policy languages, social data extraction, attack generation, visualisation, risk management methods, and initial case study results;
- TRESPASS has further strengthened its innovations with respect to the use of new visualisations, plug-and-play attacker profiles, argumentation games, and timed automata in attack navigator construction and analysis;
- 35 peer-reviewed publications and many interactive dissemination events demonstrate relevance and further increase impact potential.

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).

Results to date

At the Month 24 milestone (MS5), intermediate requirements and prototypes have been developed for the TRESPASS tools and processes. We submitted deliverables on policy languages, social data, attack generation, visualisation, risk management methods and case studies. Finally, 45 scientific publications and many dissemination events and activities were covered in the updated reports for dissemination/exploitation and standardisation.

Choices made

As in the first year, a number of fundamental choices have guided the developments in the project:

Tool chain: Based on input from the Advisory Board, the emphasis is less on a single tool chain but more on a portfolio of tools that can be tied together based on the characteristics of the case at hand. In particular, there may be multiple tools that can serve a similar purpose, for example modelling the target system or analysing and generating attack trees;

Case-specific languages: e3value has been chosen as case-specific modelling language for the money flows in the telco case. Other case-specific languages and their connections will be investigated;

Metrics: Difficulty of attack steps (control strength) is chosen as a central metric, for which cost, time required, and likelihood of success can be indicators. These parameters may depend on the chosen attacker profile;

Visualisation: The novel visualisation methods are a key innovation in themselves, while maintaining the link to the technical developments in TRESPASS. The decision to focus on attack tree simplification using spotlight and highlight techniques was based in part on feedback from the Advisory Board, analysis of the current state of the art in attack tree visualisations and in part on the state of the art in infographic techniques.

Key project results

1. We have developed a new, powerful approach to cover complex policies by combining policies and processes, enabling more advanced methods for attack generation (D1.2.1, D3.4.1).
2. We have created a structured overview of new and existing social data extraction methods for the attack navigators, as well as a process for including such data in the analyses (D2.3.1).
3. We have evaluated modelling media, resulting in the definition of a two-stage modelling approach that can combine different modalities of abstraction (D4.3.1).
4. We have evaluated different methods of visualisation, resulting in development of methods of attack tree visualisation that simplify complex attack paths (D4.2.1).
5. We have reviewed 4 international standards, 18 tool-supported risk-assessment methods and 15 tools without a specific methodology (D5.2.1).
6. Results from all three case studies include the initial modelling and visualisation of socio-technical attacks (D7.2.1, D7.3.1, D7.4.1). These results serve as input for further development of the tools and processes, for example by case-specific modelling approaches / model extensions. Demos have focused on IPTV (Year 1) and cloud (Year 2).
7. The number of accepted publications is 45 (35 being peer-reviewed) at the end of Year 2, greatly exceeding the proposed number of 20. An up-to-date list is available from the project website.
8. We have organised very successful interactive dissemination activities on data collection and data modelling, with contributions from external as well as TRESPASS participants (D9.1.4), and we have contributed to revisions of several ISO standards (D9.2.3).

Innovations

Key innovations of the TRESPASS project include:

1. New data extraction methods for social engineering and victimisation data (D2.3.1), exemplified in a social engineering experiment with physical keys (accepted for publication in the Journal of Experimental Criminology), a lost letter experiment with USB storage devices (Lastdrager, Montoya, Hartel, & Junger, 2013) and use of Eurobarometer data for victim profiles;
2. New methods for identifying risks in socio-technical systems, including the use of the e3value for identifying fraud possibilities (Ionita, Koenen, & Wieringa, 2014), and argumentation-based risk analysis (Ionita, Bullee, & Wieringa, 2014), developed by UT and used in practice by CYB.
3. Representation of metadata in terms of instructions for use (D2.3.1), enabling reasoning on the applicability of data to the target context, and associated uncertainty. For example, results of social engineering experiments would be annotated with population, sample size, link to research paper, etc.
4. The use of Timed Automata (TA) to represent attacks directly, as an alternative model for the Attack Trees and Attack-Defence trees mainly studied in Year 1 (D3.4.1).
5. Gathering social data for risk assessment by developing visualisation methods that enable social data to become tangible and interactive. This development is published in Logical Lego – Co-constructed perspectives on service design (Heath, Coles-Kemp, & Hall, 2014).
6. Based on the separation of attacker profiles and system models (Year 1 innovation), development of new attacker profiling methods and integrating the corresponding computational routines into the TRESPASS toolset (Lenin, Willemson, & Sari, 2014). We are the first to use explicit attacker profiles in attack tree analysis, enabling quick updates upon changes in the threat environment.

Having extended the TRESPASS portfolio with these scientific, artistic, and practical results and innovations, the basis for further advancing the state of the art in graph-based security models as well as security risk management in the upcoming years is excellent.

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 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

References

Heath, C., Coles-Kemp, L., & Hall, P. (2014). Logical lego – co-constructed perspectives on service design. In *Proceedings of NordDesign 2014* (p. 416). Aalto Design Factory.

Ionita, D., Bullee, J. H., & Wieringa, R. J. (2014). Argumentation-based security requirements elicitation: The next round. In *Proceedings of the 2014 IEEE 1st International Workshop on Evolving Security and Privacy Requirements Engineering (ESPRE), Karlskrona, Sweden* (pp. 7–12). IEEE Computer Society. http://eprints.eemcs.utwente.nl/25041/.

Ionita, D., Koenen, S. K., & Wieringa, R. J. (2014). *Modelling telecom fraud with e3value* (Technical Report No. TR-CTIT-14-11). Enschede: Centre for Telematics and Information Technology, University of Twente. http://eprints.eemcs.utwente.nl/25248/.

Lastdrager, E., Montoya, L., Hartel, P., & Junger, M. (2013). Applying the lost-letter technique to assess it risk behaviour. In *Proceedings of the 3rd Workshop on Socio-Technical Aspects in Security and Trust, New Orleans, USA* (pp. 2–9). USA: IEEE Computer Society. http://eprints.eemcs.utwente.nl/23424/.

Lenin, A., Willemson, J., & Sari, D. (2014, October). Attacker profiling in quantitative security assessment based on attack trees. In *19th Nordic Conference on Secure IT (NordSec), Tromsø, Norway* (Vol. 8788). Berlin: Springer.