Attack Navigator for better protection of information systems

predict
prioritise
prevent
TREsPASS

Version 0.5, 2017-05-19

As information systems become increasingly complex, keeping intruders out becomes ever more difficult. Who could be potential attackers? What tactics might they use? And which security measures will prove most effective? In order to design a systematic and effective solution, a consortium of European researchers, coordinated by the University of Twente, worked together to create the Attack Navigator. This method is the major result of the European TREsPASS project.

The right strategy

In early 2013, the researchers accepted the challenge of developing tools that would allow people to anticipate potential attacks on information systems. Investing in the right measures is worthwhile: successful attacks end up causing billions of euros of damage every year, and have a huge impact on crucial infrastructure, as well as on the economy.

The TREsPASS results complement current risk management methods by systematically analysing potential threats. “We need new methods, supported by modern technology, in order to properly identify those risks, and to consider whether we can roll out a proper countermeasure,” says project leader Pieter Hartel, professor in Cyber Security at the University of Twente.

Attack Navigator

The research resulted in the Attack Navigator: a method that builds on technical expertise and social science knowledge, combined with the use of the latest information technology and risk management processes. Smart algorithms are highly useful in pointing out what to prioritize in taking security measures.

“The complexity of technical systems, as well as the speed at which they are developed, are virtually inconceivable in full, making it nearly impossible to properly map risk scenarios. This is especially true for risks resulting from strategic actions by potential attackers,” says Hartel.

The potential attacker is the starting point for this method, which therefore expands on traditional risk management systems. The system is highly intuitive and visualizes potential routes of attackers. The process of identifying these routes starts with the engagement of the organisation. Using tangible modelling and automated extraction techniques, the map for the attack navigator is constructed, which then computes possible attacker routes. By involving stakeholders in the process of identifying potential attackers, their tactics and their targets, we obtain vital input and can increase the understanding of threats.

European context

To refine the methodology and to enable broad application, the researchers worked on five cases in different locations in Europe. For example, in the UK, they worked with a social enterprise to investigate provision of a TV-based budget planning tool for a group of people with limited financial resources, and the risks that might be involved for them in providing the service, as well as for their clients in using that service. At a telecommunications company in Germany, they looked at how complex contracts among providers themselves, as well as their clients, resulted in situations that facilitated abuse.

The TREsPASS results were evaluated positively in the final review by the European Commission, which contributed financially from the European FP7 research programme. The developed method

has a broad application range, and results in a standardized method that contributes to the prevention of incidents in Europe. It supports organizations and their clients in making informed decisions about security measures to be taken. The TREsPASS results and tools are available on-line and many of the tools are open-source.

Consortium
The TREsPASS consortium included industry partners and researchers from the social and technical sciences. Researchers from a variety of disciplines within the University of Twente contributed to the project: both from the CTIT departments of Formal Methods and Tools, Services, Cybersecurity and Safety, and Industrial Engineering and Business Information Systems (IGS).

The project partners were: BizzDesign (Netherlands), Consult Hyperion (United Kingdom), Cybernetica (Estonia), Deloitte (Netherlands), GMV SGI (Spain), GMVIS SKYSOFT (Portugal), IBM Research Zürich (Switzerland), itrust consulting s.à r.l. (Luxembourg), LUST (Netherlands), Hamburg University of Technology (Germany), Johann Wolfgang Goethe-Universität Frankfurt (Germany), Royal Holloway University of London (UK), Aalborg University (Denmark), Technical University of Denmark, University of Luxembourg, Delft University of Technology (Netherlands) and the University of Twente (Netherlands).

More information on TREsPASS and its results can be found on the website www.trespass-project.eu.
This project receives funding from the European Commission's Seventh Framework Programme under Grant Agreement No. 318003 (TREsPASS).

This project received funding from the European Commission's Seventh Framework Programme under Grant Agreement No. 318003 (TREsPASS) (click here for information from CORDIS).