predict
prioritise
prevent

TREsPASS

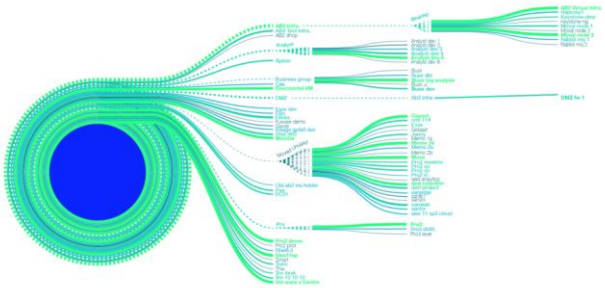
Project Newsletter

Issue 3 (July 2015)

Getting the Message Across: Visualising Security

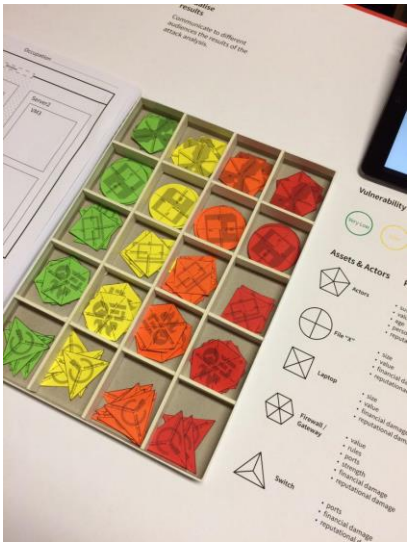
Wolter Pieters and Christian W. Probst, TREsPASS technical leaders

(images by LUST and our visualisation work package)



For security modelling and analysis, a key challenge is getting the right input for the models, and communicating the results to the stakeholders. In TREsPASS, we use the metaphor of a navigation system for both the models and associated visualisations. We have an entire work package dedicated to visualisation, including academic visualisation experts, artists, and a design studio.

The outputs of attack navigator tools can be complex and cumbersome to navigate, and the techniques developed for visualisation are an essential asset in making them understandable. In addition, visual tools help stakeholders build maps for the attack navigators, and assign parameters such as control strengths.



In this newsletter, we announce the visualisation competition, in which we ask you to help us with visualisations that capture the social and technical complexity of so-called "cyber attacks". In addition, you'll find that several research papers on visualisation have been accepted. This time, we also put some of our professors in the spotlight.

Activities and Events

July 13, 2015	The Second International Workshop on Graphical Models for Security (GraMSec), Verona, Italy.
September 8-11, 2015	TREsPASS hosts New Security Paradigms Workshop (NSPW), Twente, Netherlands.
September 15-16, 2015	Security Assessment for Systems, Services, and Infrastructures (SASSI) workshop with RASEN project, Berlin
October 21, 2015	TREsPASS visualisation competition deadline
January 13-15, 2016	TREsPASS winter school on Security in Socio-Technical Systems

Dagstuhl report

In December, Dieter Gollmann and Wolter Pieters of TREsPASS co-organised the Dagstuhl Seminar 14491 "Socio-Technical Security Metrics" with Cormac Herley, Angela Sasse and Vincent Koenig. The report of this seminar is now available. For additional details, see the previous newsletter.

CSP Forum Visualisation Workshop and Visualisation Competition

The "Security visualisation make and do" workshop @ Cybersecurity & Privacy Innovation Forum was a great success! Check out our Twitter feed (@TREsPASSProject) for some pictures. A longer report will soon be available on our website.

Continuing the theme of the workshop, **we are launching a competition for visualisations** that depict the nuances of information sharing, vulnerability and risk at the everyday level, and the enmeshed relationship between the social and technical from one of several perspectives:

- Cyber attacks on people: How your personal safety and security might be threatened by an attack on a piece of technology. What form does this attack take? How might it be experienced? What makes this attack successful?
- Cyber attacks on the State: How the security of the State might be threatened by an attack on its infrastructure. What form might an attack take? What are the impacts of such an attack? Who wins and who loses with such an attack?
- Cyber attacks on technology: How the security of technology and technologically held data might be threatened by an attack on the technology. What form might an attack take? What might make this attack successful?

Visualisations may be submitted in a number of different formats, with further details available on our website.

Selected Publications

Security analysis of socio-technical physical systems.

Gabriele Lenzini, Sjouke Mauw, Samir Ouchani

Recent initiatives that evaluate the security of physical systems with objects as assets and people as agents – here called socio-technical physical systems – have limitations: their agent behavior is too simple, they just estimate feasibility and not the likelihood of attacks, or they do estimate likelihood but on explicitly provided attacks only. We propose a model that can detect and quantify attacks. It has a rich set of agent actions with associated probability and cost. We also propose a threat model, an intruder that can misbehave and that competes with honest agents. The intruder's actions have an associated cost and are constrained to be realistic. We map our model to a probabilistic symbolic model checker and we express templates of security properties in the Probabilistic Computation Tree Logic, thus supporting automatic analysis of security properties. A use case shows the effectiveness of our approach.

http://dx.doi.org/10.1016/j.compeleceng.2015.02.019

From Cybercrime to Cyborg Crime: Botnets as Hybrid Criminal Actor-Networks

Wytske van der Wagen, Wolter Pieters

Botnets, networks of infected computers controlled by a commander, increasingly play a role in a broad range of cybercrimes. Although often studied from technological perspectives, a criminological perspective could elucidate the organizational structure of botnets and how to counteract them. Botnets, however, pose new challenges for the rather anthropocentric theoretical repertoire of criminology, as they are neither fully human nor completely machine driven. We use Actor-Network Theory (ANT) to provide a symmetrical perspective on human and non-human agency in hybrid cybercriminal networks and analyze a botnet case from this perspective. We conclude that an ANT lens is particularly suitable for shedding light on the hybrid and intertwined offending, victimization and defending processes, leading to the new concept of 'cyborg crime'.

http://dx.doi.org/10.1093/bjc/azv009

Attack Trees with Sequential Conjunction

Ravi Jhawar, Barbara Kordy, Sjouke Mauw, Saša Radomirović, Rolando Trujillo-Rasua

We provide the first formal foundation of SAND attack trees which are a popular extension of the well-known attack trees. The SAND attack tree formalism increases the expressivity of attack trees by introducing the sequential conjunctive operator SAND. This operator enables the modeling of ordered events.

We give a semantics to SAND attack trees by interpreting them as sets of series-parallel graphs and propose a complete axiomatization of this semantics. We define normal forms for SAND attack trees and a term rewriting system which allows identification of semantically equivalent trees. Finally, we formalize how to quantitatively analyze SAND attack trees using attributes.

http://dx.doi.org/10.1007/978-3-319-18467-8_23

Security-by-Experiment: Lessons from Responsible Deployment in Cyberspace

Wolter Pieters, Dina Hadžiosmanović, Francien Dechesne

Conceiving new technologies as social experiments is a means to discuss responsible deployment of technologies that may have unknown and potentially harmful side-effects. Thus far, the uncertain outcomes addressed in the paradigm of new technologies as social experiments have been mostly safety-related, meaning that potential harm is caused by the design plus accidental events in the environment. In some domains, such as cyberspace, adversarial agents (attackers) may be at least as important when it comes to undesirable effects of deployed technologies. In such cases, conditions for responsible experimentation may need to be implemented differently, as attackers behave strategically rather than probabilistically. In this contribution, we outline how adversarial aspects are already taken into account in technology deployment in the field of cyber security, and what the paradigm of new technologies as social experiments can learn from this. In particular, we show the importance of adversarial roles in social experiments with new technologies.
http://dx.doi/org/10.1007/s11948-015-9648-y

Accepted Papers

Tangible modelling to elicit domain knowledge: an experiment and focus group
Dan Ionita, Roel Wieringa, Jan-Willem Bullée, Alexandr Vasenev; *34th International Conference on Conceptual Modeling (ER 2015)*

Modeling and Analysing Socio-Technical Systems.
Zaruhi Aslanyan, Marieta G. Ivanova, Flemming Nielson, Christian W. Probst; *STPIS 2015 – 1st International Workshop on Socio-Technical Perspective in IS development.*

Examining the Contribution of Critical Visualisation to Information Security
Peter Hall, Claude Heath, Lizzie Coles-Kemp and Axel Tanner; *New Security Paradigms Workshop.*

“If you were attacked, you'd be sorry”: Counterfactuals as security arguments
Cormac Herley and Wolter Pieters; *New Security Paradigms Workshop.*

Regression Nodes: Extending attack trees with data from social sciences.
Jan-Willem Bullée, Lorena Montoya, Wolter Pieters, Marianne Junger and Pieter Hartel; *Socio-technical Aspects of Security and Trust.*

Transforming graphical system models to graphical attack models
Marieta Georgieva Ivanova, Christian W. Probst, Rene Rydhof Hansen and Florian Kammueller; *Second International Workshop on Graphical Models for Security (GraMSec)*

Attack Tree Generation by Policy Invalidation
Marieta Georgieva Ivanova, Christian W. Probst, Rene Rydhof Hansen and Florian Kammueller; *WISTP International Conference on Information Security Theory and Practice*

The navigation metaphor in security economics
Wolter Pieters, Jeroen Barendse, Margaret Ford, Claude P.R. Heath, Christian W. Probst and Ruud Verbij; *IEEE Security & Privacy magazine.*

Professor profiles

Prof.dr. Pieter Hartel is a full professor of Computer science at the University of Twente and he holds part time positions at the Technical University of Delft and at the TNO Cyber Security Lab in The Hague. He has 20 years of research and teaching experience in Cyber Security. Pieter was one of the founding fathers of the Dutch National Sentinels research program, which had a budget of over 15M Euro for scientific research. He is now building the TNO Cyber Security Cooperation for Research in The Hague, to unite the research efforts of Dutch Universities and TNO. Pieter is one of the initiators of the 3TU cyber security master, which will start in September. He has 12 years of international experience working in Switzerland, United Kingdom, United States, Malaysia, and Singapore. He is associate editor of the Crime Science Journal and reviewer for over 60 international journals, conferences, workshops and book publishers. He has supervised 19 PhD theses in 12 years, and is now the coordinator of the TREsPASS project. The vision for the project arose over a period of about 10 years of research in socio-technical modelling.

Prof.dr. Kai Rannenberg holds the Deutsche Telekom Chair (formerly T-Mobile Chair) of Mobile Business & Multilateral Security since 2002. Before that he was with the System Security Group at Microsoft Research Cambridge, UK focussing on "Personal Security Devices & Privacy Technologies". During 1993-1999 Kai worked at Freiburg University and coordinated the interdisciplinary "Kolleg Security in Communication Technology", sponsored by Gottlieb Daimler & Karl Benz Foundation researching Multilateral Security. After a Diploma in Informatics at TU Berlin he had focused his PhD at Freiburg University on IT Security Evaluation Criteria and their potential and limits regarding the protection of users and subscribers. Since 1991 Kai is active in the ISO/IEC standardization of IT Security and Criteria (JTC 1/SC 27/WG 3 "Security evaluation criteria"). Since March 2007 he is Convenor of the SC 27/WG 5 "Identity management and privacy technologies". Since September 2009 Kai is an IFIP Councillor. From May 2007 till July 2013 he chaired IFIP TC-11 "Security and Privacy Protection in Information Processing Systems", after having been its Vice-Chair since 2001. Kai is active in the Council of European Profession-

al Informatics Societies (CEPIS) chairing its Legal & Security Issues Special Interest Network (CEPIS LSI) since 2003. From July 2004 till June 2013 Kai served as the academic expert in the Management Board of the European Network and Information Security Agency, ENISA and is now a member of ENISA's Permanent Stakeholder Group . Kai`s awards include the IFIP Silver Core, the Alcatel SEL Foundation Dissertation Award and the Friedrich-August-von- Hayek-Preis of Freiburg University and Deutsche Bank. Kai's research interests include a) mobile applications and multilateral security in e.g. M-Business, M-Commerce, and LBS;b) privacy and identity management, especially attribute based authorisation; c) communication infrastructures and devices, e.g. personal security assistants and services and; d) Security and privacy standardisation, evaluation, and certification. In TREsPASS, Kai has a pivotal role as he leads the case study workpackage and is the Telco case study leader.

The Consortium

Acknowledgements

The research leading to these results has received funding from the European Union Seventh Framework Programme (FP7/2007-2013) under grant agreement n° 318003 (TREsPASS). This publication reflects only the author's views, and the Union is not liable for any use that may be made of the information contained herein.