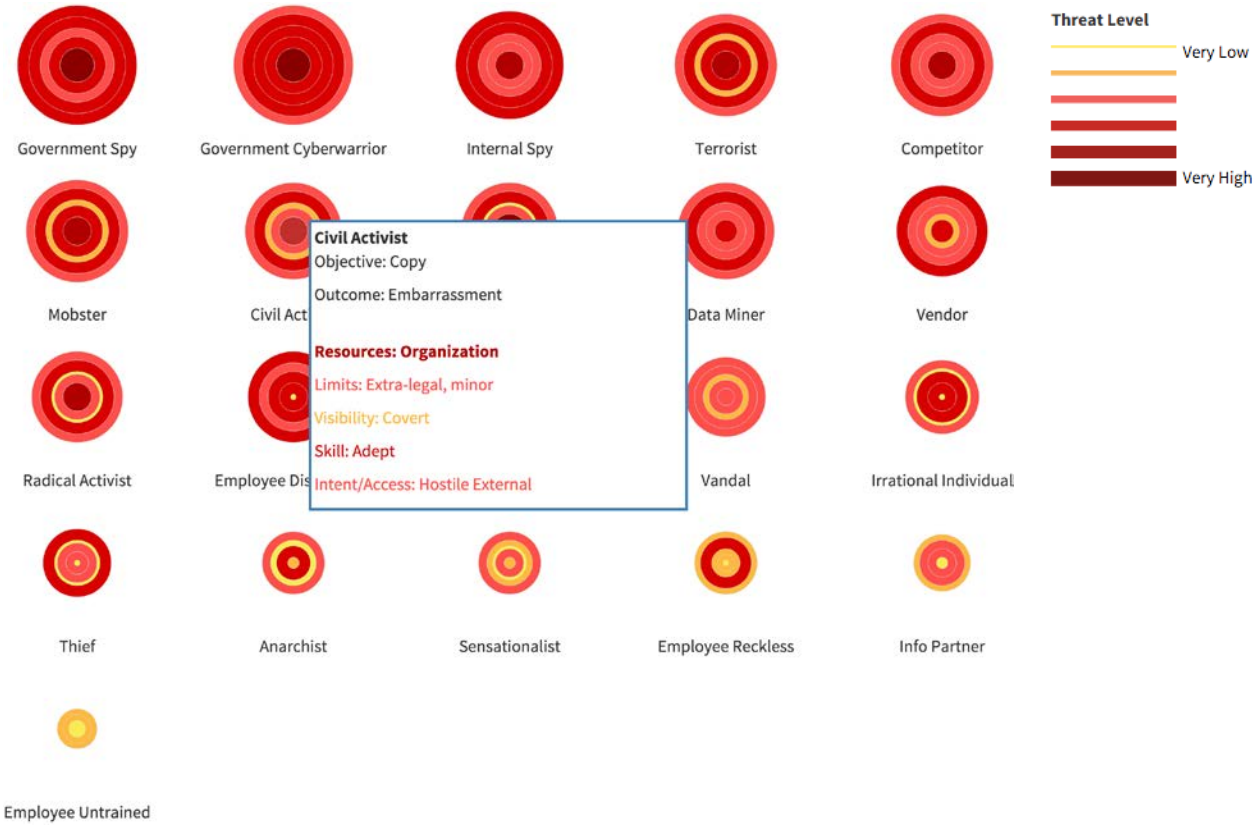
predict
prioritise
prevent
TREsPASS

Project Newsletter
Issue 4 (March 2016)

Different attackers navigate differently

Christian W. Probst - Mike Osborne, TREsPASS technical leaders



Visualisation of attacker profiles (image by LUST and our visualisation work package).

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.

During Year 3, the TREsPASS project carried out work on the topics of socio-technical security policies, models, processes, management,

extraction, sharing, analysis, visualization, prototyping and case studies, as well as 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 visualization 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.

In the first three years, 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.

Activities and Events

Future Events

April 2016	Advanced Data Collection and Risks Workshop (ADaCoR)
May 2016	Lorentz seminar on Adversarial Risk Analysis for Critical Infrastructure
June 2016	Summer school on Social Aspects of Cyber Security risk
June 2016	Graphical Models for Security workshop (GraMSec)
Nov. 2016	Dagstuhl seminar on Assessing ICT Security Risks in Socio-Technical Systems

Advanced Data Collection and Risks Workshop (ADaCoR)

This workshop is concerned: a) data collection for security incident management, b) data collection for Internet of Things and c) data protection aspects of data collection.

The programme of the workshop consists of a keynote speech, tutorials, presentation of use-cases, tools and solutions (to be identified via the call for abstracts) as well as of a panel discussion. The full programme will be available on March 5th.

The workshop will take place on April 19-21, 2016 and the venue will be University of Luxembourg. It is co-organized by Miguel Martins and Carlo Harpes from itrust as well as by Sjouke Mauw from University of Luxembourg.

Register by sending an email containing your name, surname and affiliation to adacor@itrust.lu. The workshop encourages registrations from industry actors, particularly from Luxembourg.

Summer School on Social Aspects of Cyber Security Risk

Cyber security is a truly interdisciplinary field of study that is driven by complex, real-world challenges. Because of its historical associations, the field tends to be annexed as a technological concern, but increasingly governments and organisations are recognising that cyber security risk is socially and politically constructed. This complexity makes identifying and analysing cyber security risks a significant challenge for all aspects of governance.

This Summer School will take place on June 20-23, 2016 and it seeks to explore these challenges through a combination of high profile talks on the social aspects of cyber risks and hands-on workshops to transfer a range of modelling and analytical skills innovated specifically for the cyber security terrain. The speakers will come from a range of academic disciplines including law, geography, sociology, politics and international relations, information systems and information security. We shall also feature speakers from industry and government.

This Summer School encourages registrations from PhD students and postdoctoral researchers studying the social aspects of cyber security risk. This Summer School also encourages registrations from practitioners working on real-world cyber security risk problems.

The summer school is organized by Lizzie Coles-Kemp (Royal Holloway University of London) and Peter Hall (Central St. Martins University of the Arts London). The registration's deadline is June 3, 2016. On-line registration links to appear. In the meantime, please contact Lizzie Coles-Kemp if you would like to pre-register.

Past Events

Social Engineering Award

The TREsPASS Social Engineering Award ceremony took place at the Computer Privacy and Data Protection (CPDP) conference in Brussels on January 27-29 , 2016. The jury consisted of:

- Dr. rer. nat. Zinaida Benenson (University of Erlangen-Nuremberg: leader, Human Factors in Security and Privacy Group)
- Prof. Dr. Thomas Gross (University of Newcastle upon Tyne: director, Centre for Cybercrime and Computer Security)
- Prof. Dr. Marianne Junger (University of Twente: chair, Cyber Security and Business)
- Dr. ing. Roeland van Zeijst (INTERPOL Singapore: digital crime officer; Dutch National Police: senior strategy expert)

The winner of the award was David Kelm from IT-SEAL who submitted a proposal about login credential acquisition for gaining physical access to a laptop.

The jury concluded that: "The participants provided many creative and dangerous attack ideas. Apart from the well-known social engineering principles such as authority, scarcity and liking, the authors extensively use DoS as a means of creating an emergency situation

while disrupting the business communications flow, which leads the actors into non-rational decision making. This emphasizes the importance of availability as security goal. We encourage all participants and all readers of this document to further deepen the insight of the IT security community into the social engineering threats by developing creative and practical suggestions for the scientifically sound and ethical feasibility tests of the suggested attack ideas, and by designing the corresponding countermeasures."

The winning submission by David Kelm was entitled 'Security Nightmare 2015 – Cloud Attack!'.

The second and third places went to:

- Uwe Schmalfeld (City of Nuremberg's IT department, Germany) for her proposal 'The White Knight - All's Well that Ends Well', and
- Peter Carmichael (Newcastle University, UK) for his proposal 'Social Engineering Proposal using MINDSPACE'.

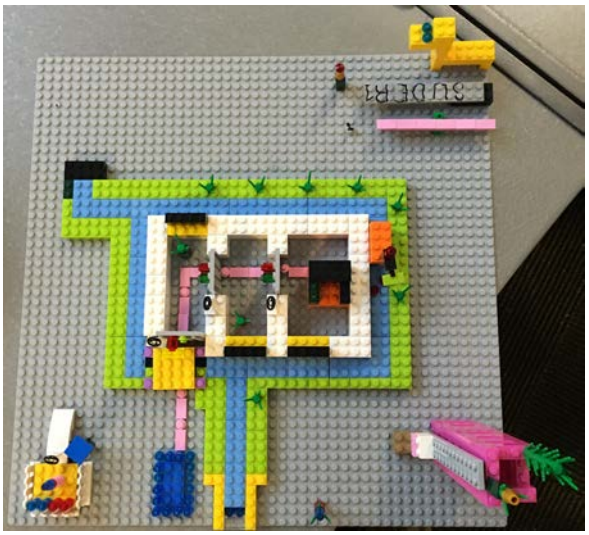
The full jury report is also available online.

Congratulations to the winners and our thanks to all the contributors!

Winter School on Security on Socio-technical Systems

At the beginning of Year 4, TREsPASS organised its first school for PhD students and practitioners. The winter school was held at the Technical University of Denmark (DTU) from January 13-15, 2016 and attracted 12 Ph.D. students and 5 practitioners from Finland, Germany, the Netherlands, Denmark, Luxembourg, Poland, Italy and India.

The winter school featured courses by international experts in the area of Internet voting and socio-technical systems. The courses illustrated the challenges in analysing and guaranteeing security in socio-technical systems, using Internet voting as an example of such systems, partly disseminating the TREsPASS results, and partly relating it to other research areas. As part of the practical exercises, participants modelled a cloud infrastructure as part of a potential Internet voting system, and identified possible attacks on it.



DTU plans to run a similar school in summer 2017.

New Security Paradigms Workshop (NSPW)

NSPW offers a unique forum for information security research involving high-risk, high-opportunity paradigms, perspectives, and positions. TREsPASS had a big presence at last year's event (September 8-11, 2015) in De Lutte, The Netherlands. The event was co-organized by University of Twente's Lorena Montoya and in addition, 3 out of the 12 papers presented were (co)authored by TREsPASS researchers. The full list of papers is available in the ACM website. The call for papers for the next edition, which will take place on Sept. 26-29, 2016 in Colorado, USA has been already launched.

Graphical Models for Security Workshop (GraMSec)

TREsPASS makes use of various graphical models and approaches: from socio-technical models to attack models. GraMSec was set up by University of Luxembourg as a platform for community building. GraMSec aims to contribute to the development of well-founded graphical security models, efficient algorithms for their analysis, methodologies for their practical use, and to serve as a forum for security researchers and practitioners to share their insights and experiences in graphical security models.

The 2nd edition of GraMSec took place in Verona, Italy on July 13, 2015, was co-organized by University of Luxembourg's Sjouke Mauw and was co-located with the prestigious IEEE Computer Security Foundations (CSF) Symposium. The invited speaker, Marc Bouissou (Ecole Centrale Paris and EDF R&D France) gave a talk about dynamic graphical models for joint modelling of security and safety.

Post-proceedings of GraMSec'2015 are now available. Two of six papers accepted to the workshop were from TREsPASS researchers. Moreover, the post-proceedings also include an invited paper on the Attack Navigator jointly produced by TREsPASS partners.

An important outcome of the workshop was a bilateral project between IRISA (France) and University of Luxembourg (Luxembourg) which is currently under submission.

The call for papers for the next GraMSec, to be held on June 27, 2016 in Lisbon, Portugal (also co-located with IEEE CSF) has been already launched. We encourage submissions from the community.

Security Assessment for Systems, Services and Infrastructures (SASSI)

The SASSI workshop took place on September 15-16, 2015 and provided a forum to discuss innovative approaches to security assessment, security testing and security certification for software-based systems. Experts from industry and academia presented and discussed their solutions to key issues such as legal-risk analysis, security risk analysis, risk-based engineering, vulnerability testing, model based security testing, standardization, and certification. The workshop had a special focus on the interaction between innovations and industrial requirements, especially when security meets the demands of cost efficiency and scalability. The contributions originated from industrial practice and are complemented by industry grade research results from national and international research projects. SASSI was co-organised by Jan Willemson and Christian W. Probst from TREsPASS partners Cybernetica and the Technical University of Denmark.

Border Sessions

Border Sessions explores how emerging technologies shape our future society and meet the innovators who are making it happen. TREsPASS ran two sessions as part of the 2015 edition.

Focusing on the work that TREsPASS has undertaken in privacy risks in health and social care, TREsPASS ran a hack and visualisation session on privacy risks on the morning of November 11, 2015. This session was particularly designed for SMEs working in health and social care who have to identify and communicate technology risks.

The theme of privacy risks in health and social care continued in the afternoon when TREsPASS hosted the TREsPASS visualisation competition awards. The keynote for this session was given by Joe Reddington from Royal Holloway University of London, who talked about accounting for multi-stakeholder risks in healthcare design.

International Association of Societies of Design Research (IASDR)

Royal Holloway University of London's Claude Heath and Peter Hall took part in a creative security workshop at the Interplay Conference in Brisbane on November 2, 2015. Claude Heath showcased some of the TREsPASS visualisation research and ran a LEGO modelling workshop using TREsPASS analogue modelling methods.

Publications

Selected Publications

Attack Tree Generation by Policy Invalidation

Marieta Georgieva Ivanova, Christian W. Probst, René Rydhof Hansen and Florian Kammüuller

Attacks on systems and organisations increasingly exploit human actors, for example through social engineering, complicating their formal treatment and automatic identification. Formalisation of human behaviour is difficult at best, and attacks on socio-technical systems are still mostly identified through brainstorming of experts. In this work we formalize attack tree generation including human factors; based on recent advances in system models we develop a technique to identify possible attacks analytically, including technical and human factors. Our systematic attack generation is based on invalidating policies in the system model by identifying possible sequences of actions that lead to an attack. The generated attacks are precise enough to illustrate the threat, and they are general enough to hide the details of individual steps.
http://dx.doi.org/10.1007/978-3-319-24018-3_16

Telephone-based social engineering attacks: An experiment testing the success and time decay of an intervention

Jan-Willem Bullée, Lorena Montoya, Marianne Junger and Pieter Hartel

The objective of this study is to evaluate the effectiveness of an information campaign to counter a social engineering attack via the telephone. Four different offenders phoned 48 employees and made them believe that their PC was distributing spam emails. Targets were told that this situation could be solved by downloading and executing software from a website (i.e. an untrusted one). A total of 46.15 % of employees not exposed to the intervention followed the instructions of the offender. This was significantly different to those exposed to an intervention 1 week prior to the attack (9.1 %); however there was no effect for those exposed to an intervention 2 weeks prior to the attack (54.6 %). This research suggests that scam awareness-raising campaigns reduce vulnerability only in the short term.
http://dx.doi.org/10.3233/978-1-61499-617-0-107

Examining the Contribution of Critical Visualisation to Information Security

Peter Hall, Claude Heath, Lizzie Coes-Kemp and Axel Tanner

This paper examines the use of visualisations in the field of information security and in particular focuses on the practice of information security risk assessment. We examine the current roles of information security visualisations and place these roles in the wider information visualisation discourse.

We present an analytic lens which divides visualisations into three categories: journalistic, scientific and critical visualisations. We then present a case study that uses these three cat-

egories of visualisations to further support information security practice. Two significant results emerge from this case study: (1) visualisations that promote critical thinking and reflection (a form of critical visualisation) support the multi-stakeholder nature of risk assessment and (2) a preparatory stage in risk assessment is sometimes needed by service designers in order to establish the service design before conducting a formal risk assessment. The reader is invited to explore the images in the digital version of this paper where they can zoom in to particular aspects of the images and view the images in colour.
http://dx.doi.org/10.1145/2841113.2841118

Using Value Models for Business Risk Analysis in e-Service Networks

Dan Ionita, Roel Wieringa, Lars Wolos, Jaap Gordijn and Wolter Pieters.

Commercially provided electronic services commonly operate on top of a complex, highly-interconnected infrastructure, which provides a multitude of entry points for attackers. Providers of e-services also operate in dynamic, highly competitive markets, which provides fertile ground for fraud. Before a business idea to provide commercial e-services is implemented in practice, it should therefore be analysed on its fraud potential.

This analysis is a risk assessment process, in which risks are ordered on severity and the unacceptable ones are mitigated. Mitigations may consist of changes in the e-service network to reduce the attractiveness of fraud for the fraudster, or changes in coordination process steps or IT architecture elements to make fraud harder or better detectable.

We propose to use e3 *value* business value models for the identification and quantification of risks associated with e-service packages. This allows for impact estimation as well as understanding the attacker's business cases. We show how the e3 *value* ontology — with minimal extensions – can be used to analyse known telecommunication fraud scenarios. We also show how the approach can be used to quantify infrastructure risks. Based on the results, as well as feedback from practitioners, we discuss the scope and limits of generalizability of our approach.
http://dx.doi.org/10.1007/978-3-319-25897-3_16

Accepted Publications

Modeling and Verification of Insider Threats; Using Logical Analysis. Florian Kammueller, F. and Christian W. Probst; *IEEE Systems Journal.*

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.*

The Value of Attack-Defence Diagrams. Holger Hermanns, Julia Kramer, Jan Krcal, and Marielle Stoelinga; *ETAPS/post.*

Automated identification and prioritization of business risks in e-service networks. Dan Ionita, Roel J. Wieringa and Jaap Gordijn; *8th IFIP WG 8.1. Working Conference on the Practice of Enterprise Modelling* (PoEM 2015).

PhD Student Showcase

Sven M. Hallberg – Hamburg University of Technology

After some years working as a software developer in the IT security field, **Sven M. Hallberg** earned a diploma in mathematics (Dipl.-Math.) from the University of Hamburg where he studied algebra and wrote his thesis on cryptographic identification schemes. Sven is now pursuing a doctoral degree at TUHH, applying modern security research to cyber-physical systems. His interests include approaches based on languages and language theory as well as formal logic. He brings his mathematical and software engineering background to TREsPASS to aid with statistical analysis as well as process integration.

Ahmed Seid Yesuf - Goethe University Frankfurt

Ahmed Seid Yesuf obtained a bachelor degree with distinction on Computer Science and IT from Haramaya University, Ethiopia in 2009. Furthermore, he obtained his M.Sc. degree in computer science (Informatics) with specialisation on Design and Engineering in 2013 from Trento University, Italy. His master thesis dealt with the implementation of a framework for a context-aware and computer-aided attack tree modelling approach for software development. He did his internship and MSc. thesis at SAP Next Business and Research Karlsruhe, Germany.

Since November 2013, he works as PhD student, research & teaching assistant at the chair of Mobile Business and Multilateral Security at Johann Wolfgang Goethe University in Frankfurt (Germany). In TREsPASS he is mainly involved in the case studies. His PhD topic focuses on a risk preventive approach of tele-

communication services. Generally he is interested in risk modelling approaches, system security, design and requirement engineering, usability of system security approaches, and secure software development.

Jan-Willem Bullée – University of Twente

Jan-Willem Bullée studied both Computer Science and Psychology at the University of Twente. In his master project, he combined the two disciplines to find emerging leadership in small groups based on visually observable behaviour.

In January 2013 Jan-Willem joined the TREsPASS project as Ph.D. candidate, where he is mainly involved in the work packages dealing with model specification and the data management process.

His research interests include persuasion and deception in the context of cybercrime.

In TREsPASS he uses experiments to gain insight into the behaviour of target and offender, and the preventive measures against fraudulent offences, in particular against social engineering.

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.