predict
prioritise
prevent

TREsPASS

Project Newsletter

Issue 2 (February 2015)

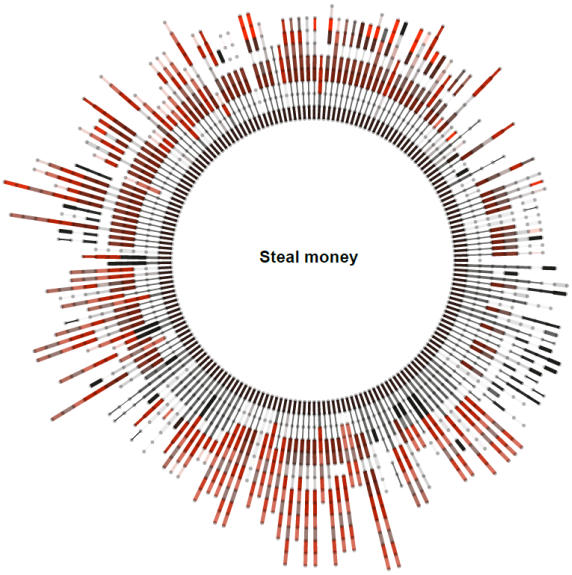
Key results of the first two years

Wolter Pieters and Christian W. Probst, TREsPASS technical leaders

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.

TREsPASS will be organising and attending many events in 2015. In particular, check out our visualization workshop at the CSP Forum, the joint SASSI workshop with the RASEN project, and the GraMSec and NSPW scientific workshops that we host.

Open Calls

GraMSec 2015

GRAPHICAL MODELS FOR SECURITY

July 13, 2015, Verona, Italy
Co-located with CSF 2015
http://www.gramsec.uni.lu/

SCOPE

Graphical security models provide an intuitive but systematic methodology to analyze security weaknesses of systems and to evaluate potential protection measures. Formal methods and computer security researchers, as well as security professionals from industry and government, have proposed various graphical security modeling schemes. Such models are used to capture different security facets (digital, physical, and social) and address a range of challenges including security assessment, risk analysis, automated defensing, secure services composition, policy validation and verification. The objective of GraMSec is to contribute to the development of well-founded graphical security models, efficient algorithms for their analysis, as well as methodologies for their practical usage.

TOPICS

The workshop seeks submissions from academia, industry, and government presenting novel research on all theoretical and practical aspects of graphical models for security. Topics include, but are not limited to:

- Attack trees, attack graphs, and their variants
- Petri nets, Markov chains, and Bayesian networks for security
- UML-based models and other graphical modeling approaches for security
- Enhancement and/or optimization of existing graphical security models
- Methods for (semi-)automatic generation of graphical security models
- Scalability of graphical security models
- Software tools for graphical security modeling and analysis
- Risk assessment and risk management using graphical security models
- Methods for quantitative analysis of graphical security models
- Formal semantics of graphical security models
- Formal verification of graphical security models
- Game theoretical approaches to graphical security models
- Visualization of system security
- Visual security modeling and analysis of socio-technical and cyber-physical systems
- Graphical models for system, organizational, and business security
- Graphical security models for emerging paradigms (e.g., Cloud computing, IoT, Software Defined Networks, Big Data)
- Case studies and experience reports on the use of graphical security modeling paradigm.

IMPORTANT DATES

- Submission deadline: April 19, 2015
- Acceptance notification: May 26, 2015
- Camera ready version: June 15, 2015
- Workshop: July 13, 2015

NSPW 2015

NEW SECURITY PARADIGMS WORKSHOP

September 8–11, 2015
Twente, The Netherlands
www.nspw.org

SCOPE

Since 1992, the New Security Paradigms Workshop (NSPW) has offered a unique forum for computer security/information security research involving high-risk, high-opportunity paradigms, perspectives and positions. NSPW seeks embryonic, disruptive, and unconventional ideas that benefit from early feedback. The ideas are almost always not yet proven, and sometimes infeasible to validate to the extent expected in traditional forums. Submissions typically address current limitations of computer/information security, directly challenge long-held beliefs or the very foundations of security, or view problems from an entirely novel angle leading to new solution paradigms. NSPW seeks ideas pushing the boundaries of science and engineering beyond what would typically be considered mainstream; papers that would be strong candidates in "conventional" computer/information security venues are, as a rule of thumb, a poor fit for NSPW. We welcome papers with perspectives that augment traditional computer/information security, both from other computer science disciplines and other sciences that study adversarial relationships (e.g., biology, economics, the social sciences). For NSPW 2015, we especially welcome papers from first-time NSPW authors. The workshop itself is highly interactive with presentations by authors prepared for in-depth discussions, and ample opportunity to exchange views with open-minded peers. NSPW is also distinguished by its deep-rooted tradition of positive feedback, collegiality, and encouragement.

TOPICS

REGULAR SUBMISSIONS (6–15 pages): NSPW papers vary in format and style, but often involve a systematic investigation supported by structured argument. Some involve an opinionated analysis, or explore a design space that emerges upon replacing a common assumption (even if this is beyond current technology). Successful submissions show strong scholarship, demonstrate sound knowledge of related literature while placing the contributions in context to it, and are often accompanied by suitable forms of early validation and a research agenda for broader validation. Ideal papers lead to spirited workshop discussion, but NSPW is not a debating society — the spirited discussion should relate to new ideas and perspectives as characterized above, rather than well-known controversial topics.

IMPORTANT DATES

- Submissions: April 18, 2015 23:59 (UTC-0, UK time) firm
- Acceptance notification: June 11, 2015
- Pre-proceedings deadline: August 3, 2015 (ACM SIG formatting required, Option 1)
- Workshop: September 8–11, 2015, Twente, The Netherlands
- Post-proceedings manuscripts: November 3, 2015

Calendar of Activities

April 28-29, 2015	TREsPASS visualisation workshop @ CSP Forum, Brussels. http://www.cspforum.eu/2015
July 13, 2015	GraMSec workshop, Verona, Italy. http://www.gramsec.uni.lu/
September 8-11, 2015	TREsPASS hosts New Security Paradigms Workshop (NSPW), Twente, Netherlands. www.nspw.org
September 15-16, 2015	Security Assessment for Systems, Services, and Infrastructures (SASSI) workshop with RASEN project, Berlin http://www.fokus.fraunhofer.de/go/sassi15

Past Events

Social Engineering Award

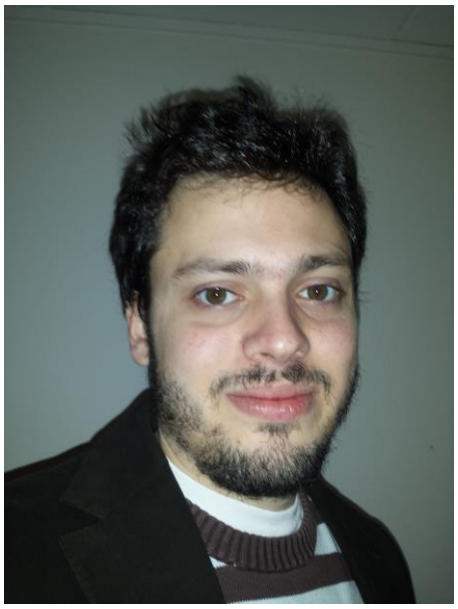
On January 22, the TREsPASS Social Engineering Award ceremony took place at the Computer Privacy and Data Protection conference in Brussels. The jury announced that the EUR 750 prize goes to.... Demetris Antoniou! Congratulations!

From the jury report:

"His proposal, *It is all about the individual*, in form pays homage to the way emeritus hacker Kevin Mitnick warns his audience about security threats. Catchingly written, Antoniou's proposal is original, feasible and extremely threatening to the victim company involved. In his entry, the author combines a number of known techniques to prey on exactly the responsible nature of perhaps the most socially-engaged employees.

The core attack vector is that company workers are sought out on their charity involvement and are time-pressured into (unwittingly) installing malware on the network. Not, as often seen, by targeting people's curiosity or wallet, but rather their heart, identity and sense of responsibility. With a high-value target, medium investment and low risk-ratio, we find it an elegant and attractive attack for (industrial) espionage.

As the paper discusses, countermeasures are very costly. Besides strict technical measures, the company should strengthen its selection process, enforce permanent awareness and perhaps maintain online honeypots. These costly procedures would also have legal and ethical consequences. While national security agencies might have the time and resources, for most companies this would be just too much to ask. Well done!"



We'd like to thank the jury, consisting of Marianne Junger, Roeland van Zeijst and Zinaida Benensen for their great work, and of course all the participants for the very interesting submissions.

Dagstuhl

Dieter Gollmann and Wolter Pieters of TREsPASS co-organised the Dagstuhl Seminar 14491 "Socio-Technical Security Metrics". The other organisers were Cormac Herley, Angela Sasse and Vincent Koenig. The seminar took place in the first week of December.

Socio-technical security metrics are essential for attack navigators, but how to define, collect, and use them? Safety metrics inform many decisions, from the height of new dikes to the design of nuclear plants. We can state, for example, that the dikes should be high enough to guarantee that a particular area will flood at most once every 1000 years. Even when considering the limitations of such numbers, they are useful in guiding policy. Metrics for the security of information systems have not reached the same maturity level. This is partly due to the nature of security risk, in which an adaptive attacker rather than nature causes the threat events. Moreover, whereas the human factor may complicate safety and security procedures alike, in security this "weakest link" may be actively exploited by an attacker, such as in phishing or social engineering. In order to measure security, one therefore needs to compare online hacking against such social manipulations, since the attacker may simply take the easiest path.

In this seminar, we searched for suitable metrics that allow us to estimate information security risk in a socio-technical context, as well as the costs and effectiveness of countermeasures. Working groups addressed different topics, including security as a science, testing and evaluation, social dynamics, models and economics. The working groups focused on three main questions: what are we interested in, how to measure it, and what to do with the metrics.

The full report is currently being written, and will be made available as Dagstuhl Report.

Industry workshops

A TREsPASS workshop "Data collection for cyber and social risk assessment" was held in Lisbon 24-26 September 2014. The aim of the workshop was to identify resources and processes for collecting data that can be used to estimate risks. The data management process plays a central role in TREsPASS by combining information from different sources into a consistent data model, to support risk assessment that covers technical (digital), social and physical environment in the organisations.

Combining various data domains: technical (e.g., specification of IT infrastructure), social (e.g., attacker and victim behavioural patterns), physical (e.g., building description), represents a major challenge to predict, prioritise and prevent potential threats. The focus of the workshop was to discuss practical difficulties in collecting, classifying and interpreting data from different domains. On the one hand, the project team shared the developments and innovations developed by the project with industrial participants. On the other hand, the project team learned from the expertise of the invited companies and governmental authorities. In particular, external participants of the workshop significantly contributed with experiences from their own organisation and communities. The workshop was attended by 30 participants and lasted for three days, more than half being external to the project. The participants, invited by the organising partner GMV Portugal, work on risk management in areas related to the project's research topics and case studies.

A workshop titled "Data Modelling for cyber and social risk assessment" and organised by IBM was held in Zürich on November 17-18 2014. The workshop focused on basic modelling techniques and was designed to field-test project ideas on how to build and analyse models, with emphasis on the structure of the models and the type of information captured.

PhD Student Showcase

Sven Übelacker – Hamburg University of Technology

Sven Uebelacker studied mathematical economics (Dipl-Math.oec.) at the Universities of Hildesheim, Balearic Islands and Ulm with a focus on computer and actuarial science. After working at computer centers of the University of Applied Science in Munich and later of the Hamburg University of Technology in the area of computer security, he started at DFN-CERT, a company assuring the security of Germany's national research and education network DFN.

In March 2013 he came back to the Hamburg University of Technology in order to contribute to the EU FP7 research project TREsPASS. He is interested in human factors especially how employees become susceptible to Social Engineering attacks.

Lars Wolos – Goethe University Frankfurt

Lars Wolos holds a diploma in business administration (Dipl.-Kfm.) from Goethe University in Frankfurt, Germany. After focusing on Business Informatics during his studies and with a strong background in telecommunications, he started working at the Chair of Mobile Business & Multilateral Security as research & teaching assistant and PhD student in 2010. His research interests focus on telecommunication service design, notably understanding how misuse potential correlates with service design, as opportunities to commit fraud are often enabled by design flaws. He has been working on the EU FP7 research project TREsPASS from its start, in particular the telecommunications case study.

Selected Publications

DAG-Based Attack and Defense Modeling: Don't Miss the Forest for the Attack Trees.

Barbara Kordy, Ludovic Piètre-Cambacédès, Patrick Schweitzer

This paper presents the current state of the art on *attack and defense modeling approaches that are based on directed acyclic graphs (DAGs)*. DAGs allow for a hierarchical decomposition of complex scenarios into simple, easily understandable and quantifiable actions. Methods based on threat trees and Bayesian networks are two well-known approaches to security modeling. However there exist more than 30 DAG-based methodologies, each having different features and goals.
The objective of this survey is to summarize the existing methodologies, compare their features, and propose a taxonomy of the described formalisms. This article also supports the selection of an adequate modeling technique depending on user requirements.
http://dx.doi.org/10.1016/j.cosrev.2014.07.001

Experimenting with Incentives: Security in Pilots for Future Grids.

Francien Dechesne, Dina Hadziosmanovic, Wolter Pieters

Electricity grids are in a transition phase. With the rise of renewable energy, energy "prosumers," and electric vehicles, traditional models of matching supply and demand are no longer adequate. Grid pilot projects can help identify ways to improve cybersecurity in future grids.
http://dx.doi.org/10.1109/MSP.2014.115

Cloud Radar: Near Real-Time Detection of Security Failures in Dynamic Virtualized Infrastructures.

Sören Bleikertz, Carsten Vogel, Thomas Groß

Cloud infrastructures are designed to share physical resources among many different tenants while ensuring overall secu rity and tenant isolation. The complexity of dynamically changing and growing cloud environments, as well as insider attacks, can lead to misconfigurations that ultimately result in security failures. The detection of these misconfigurations and subsequent failures is a crucial challenge for cloud providers—an insurmountable challenge without tools.
We establish an automated security analysis of dynamic virtualized infrastructures that detects misconfigurations and security failures in near real-time. The key is a systematic, differential approach that detects changes in the infrastructure and uses those changes to update its analysis, rather than performing one from scratch. Our system, called Cloud Radar, monitors virtualized infrastructures for changes, up- dates a graph model representation of the infrastructure, and also maintains a dynamic information flow graph to determine isolation properties. Whereas existing research in this area performs analyses on static snapshots of such infrastructures, our change-based approach yields significant performance improvements as demonstrated with our proto- type for VMware environments.
http://eprints.eemcs.utwente.nl/25124/

Limiting Adversarial Budget in Quantitative Security Assessment.

Aleksandr Lenin, Ahto Buldas

We present the results of research of limiting adversarial budget in attack games, and, in particular, in the failure-free attack tree models presented by Buldas-Stepanenko in 2012 and improved in 2013 by Buldas and Lenin. In the previously presented models attacker's budget was assumed to be unlimited. It is natural to assume that the adversarial budget is limited and such an assumption would allow us to model the adversarial decision making more close to the one that might happen in real life. We analyze three atomic cases – the single atomic case, the atomic AND, and the atomic OR. Even these elementary cases become quite complex, at the same time, limiting adversarial budget does not seem to provide any better or more precise results compared to the failure-free models. For the limited model analysis results to be reliable, it is required that the adversarial reward is estimated with high precision, probably not achievable by providing expert estimations for the quantitative annotations on the attack steps, such as the cost or the success probability. It is doubtful that it is reasonable to face this complexity, as the failure-free model provides reliable upper bounds, being at the same time computationally less complex.

http://dx.doi.org/10.1007/978-3-319-12601-2_9

The persuasion and security awareness experiment: reducing the success of social engineering attacks.

Jan-Willem Bullée, Lorena Montoya, Wolter Pieters, Marianne Junger, Pieter Hartel

Objectives: The aim of the current study is to explore to what extent an intervention reduces the effects of social engineering (e.g. the obtaining of access by persuasion) in an office environment. In particular, we study the effect of authority during a `social engineering' attack.

Methods: 31 different `offenders' visited the offices of 118 employees and on the basis of a script, asked them to hand over their office keys. Authority, one of the six principles of persuasion, was used by half of the offenders to persuade a target to comply with his/her request. Prior to the visit, an intervention was randomly administered to half of the targets to increase their resilience against attempts by others to obtain their credentials.

Results: 37.0% of the employees who were exposed to the intervention surrendered their keys whilst 62.5% of those who were not exposed to it handed it over. The intervention has a significant effect on compliance but the same was not the case for authority.

Conclusions: Awareness-raising about the dangers, characteristics and countermeasures associated with social engineering proved to have a significant positive effect on neutralizing the attacker.

http://dx.doi.org/10.1007/s11292-014-9222-7

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.