predict
prioritise
prevent
TREsPASS

Project Newsletter
Issue 1 (October 2014)

Attack navigators for socio-technical cyber risk assessment

Wolter Pieters and Christian W. Probst, TREsPASS technical leaders

In the cyber age, assessing the risk of an attacker penetrating one's IT infrastructures is essential. However, organisations often struggle with integrating the role of people and social structures into the analysis. How can one understand the difference in risk posed by a bored college graduate, versus a well-financed organisation trolling for valuable intellectual property?

The TREsPASS consortium is developing attack navigators to assist organisations in their cyber security risk assessments. We believe that the best question to ask in cyber security risk assessment is how hard something is, before discussing probabilities. How hard something is can, for example, be expressed in terms of the time it is expected to take, which can be done for digital, physical, as well as social attack steps.

We use maps (mathematically: graphs) to investigate this question, basically calculating optimal routes as done in car navigation. We are able to do this for different types of attackers with different skills and resources, enabling what we call "plug-and-play attackers". With the same model, we can evaluate risks assuming script kiddies or foreign security agencies as attackers.

Our visualisation experts have made invaluable contributions to the usability of the TREsPASS framework and tools. They are working not only with digital forms of visualisation, but also physical ones, including Lego building blocks.

Apart from providing quantitative analysis features, the attack navigators also serve as "thinking tools". One of our case-study end users said: "I just wanted to thank you for the excellent session you ran for us this morning; very complex and in depth but incredibly useful! Mapping out where we are, where we want to go, how we'll get there clarifies all sorts of things."

Key TREsPASS staff is present at conferences worldwide to inform you about our latest research results. If you wish to showcase your own results at one of our events, check out our call for the Security Nightmare 2014 / Cybercrime Social-Engineering Analysis Challenge in this newsletter.

Calendar of Activities

November 6, 2014	Lorena Montoya will present the results of the “May I Have Your Key” experiment at the National Conference of Building Automation in Hilversum, The Netherlands.
November 12-13, 2014	LUST, University of Twente, TU Delft, IBM and Royal Holloway will present TREsPASS results and visualisations at Border Sessions technology festival, The Hague, Netherlands.
November 17-18, 2014	TRE$_S$PASS workshop on basic modelling techniques for attack navigators, Zürich, Switzerland.
November 30-December 5, 2014	Dagstuhl seminar on Socio-Technical Security Metrics, organized by Wolter Pieters, Dieter Gollmann, M. Eric Johnson, Vincent Koenig and Angela Sasse. The seminar is by invitation only, but expressions of interest are welcome (no guarantees).
January 21-23, 2014	Cybercrime Social Engineering Analysis Challenge; Computers, Privacy and Data Protection Conference, Brussels, Belgium (see call below).

Open Calls

Security Nightmare 2014
Cybercrime Social-Engineering Analysis Challenge

TREsPASS invites you to the Social Engineering Challenge 2014. You can apply by submitting your proposal before December 1st. After selection by a professional jury, the award winning proposal will be announced at the CPDP conference in Brussels, Belgium, on January 21-23, 2015.

Cybercrime is increasing rapidly all around the globe. Methods such as phishing, scamming, and hacking are becoming more sophisticated. To counteract this pervasive problem, organisations have investigated technical solutions as well as awareness programs for employees and customers. As Social Engineering is a key factor in 92% of industrial espionage attacks (Verizon), the human factor is attracting increasing media attention . However, systematic analysis of the Social Engineering problem is still rare, and scientists and practitioners from diverse research disciplines are trying to understand the mechanisms behind it more holistically. You can help! You are invited to think of attack scenarios, that might be used to bypass existing security controls. Tricking the human element of security is what this challenge is about: the ultimate security nightmare. We are **not** looking for new hacking tools, spam bots, phishing attacks, blackmail, etc. To stimulate your creativity, you may wish to visit this page: Social Engineering Panel. Could you think of a comparable or better scenario? For example, one in which the use of security tokens is bypassed? Or how credit card information can be obtained without the use of a PC?

Describe your Social Engineering attack idea and include a suitable countermeasure to prevent your scenario from taking place: think of policies, access controls, etc. It would be ideal if you also provide a short outline of an experiment/research proposal that could be used to test the feasibility or relevance of your attack scenario.

Submit your 2-page proposal and a 1-page CV before December 1st 2014 to www.easychair.org/conferences/?conf=trespassec14.

The proposals will be evaluated and judged based on creativity, feasibility and deceivability. The best proposal will be awarded with €750 and the winner will be invited to the CPDP 2015 conference to receive the award. A maximum of €800 travel costs will be reimbursed.

Good luck,

TREsPASS project.

Disclaimer:
Please check the terms and conditions at www.trespass-project.eu/award. We are collecting input for research and dissemination purposes, so please make sure that the information provided is non-confidential.

Past Events

GraMSec 2014

TREsPASS co-organised The First International Workshop on Graphical Models for Security (GraMSec'14). The workshop was held in Grenoble, France, on April 12, 2014, as one of the satellite events of The European Joint Conferences on Theory and Practice of Software (ETAPS) 2014. Graphical security models provide an intuitive but systematic methodology to analyze security weaknesses of systems and to evaluate potential protection measures. Such models have been subject of academic research and have also been widely accepted by the industrial sector as a means to support and facilitate threat analysis and risk management processes. The objective of the International Workshop on Graphical Models for Security is to contribute to the development of well-founded graphical security models, efficient algorithms for their analysis, and also methodologies for their practical usage. The aim of the workshops is to bring together academic researchers and industry practitioners designing and using visual models for security and to provide a platform for discussion, knowledge exchange and collaborations.

Thirteen submissions were received for this first edition of GraMSec, of which six were accepted:

- Erlend Andreas Gjære and Per Håkon Meland **Threats Management Throughout the Software Service Life-cycle** [slides]
- Ludovic Apvrille and Yves Roudier **Towards the Model-Driven Engineering of Secure yet Safe Embedded Systems** [slides] [TTool]
- Thomas Bauereiss and Dieter Hutter **Possibilistic Information Flow Control for Workflow Management Systems** [slides]
- Stéphane Paul **Towards Automating the Construction & Maintenance of Attack Trees: a Feasibility Study** [slides]
- Cristian Prisacariu **Actor Network Procedures as Psi-calculi for Security Ceremonies**
- Aitor Couce Vieira, Siv Hilde Houmb, and David Rios Insua **A Graphical Adversarial Risk Analysis Model for Oil and Gas Drilling Cybersecurity**

In addition, we had an excellent keynote presentation by Ketil Stølen. We would like to thank all authors for submitting their work to GraMSec'14, and the members of the Program Committee as well as the external reviewers for their efforts and high-quality reviews. We are also grateful to the organizers of ETAPS 2014, especially to the Workshops Chair Axel Legay, for accepting GraMSec'14 as an ETAPS-affiliated event and for providing a perfect environment for running the workshop. We would like to thank the Fonds National de la Recherche Luxembourg and the European Commission's Seventh Framework Programme for their partial sponsorship of the workshop (FNR-CORE ADT2P grant and the EU FP7 grant no. 318003 TREsPASS). Finally, we are thankful to the University of Luxembourg, the University of Twente, and Delft University of Technology for their contributions in kind to GraMSec'14.

PhD Student Showcase

Dan Ionita – University of Twente

My name is Dan Ionita and I come from Romania, more specifically, from the capital of Bucharest. I completed my B.Sc. in Management Engineering in the field of Electrical Engineering, Telecommunications and IT at the Polytechnic University of Bucharest. Currently I am completing a M.Sc. in Computer Science, specializing in Information Systems Engineering. I have some experience with networks, databases and web design. My main research interests are related to Information Systems and Business IT. Within TREsPASS, I will work as a PhD student at the UT and I expect my main contributions to revolve around WP5 and WP7: Risk-Assessment and Case Studies, with more specific research topics hopefully including: identifying vulnerabilities, insider threats and hybrid attack paths, system architectures and specification, as well as modelling and also requirements engineering. In my free time, I like to go skiing or swimming, depending on the season. Other (indoor) hobbies include working with computers (programming, web design, computer games) and drinking beer with my friends.

Zaruhi Aslanyan – Technical University of Denmark

My name is Zaruhi Aslanyan. Currently I am a research assistant in the Technical University of Denmark, which I joined in February. I obtained my BSc and MSc in Informatics and Applied Mathematics from Yerevan State University. After finishing MSc in my home country, Armenia, I had the goal to extend and develop my professional knowledge and skills by exploring the experience of other countries. That is why I continued my study in Computer Science at Blekinge Tekniska Högskola, Sweden. While studying at Blekinge Tekniska Högskola, I participated in an Erasmus exchange student program at the Vrije University Amsterdam, The Netherlands, for five months. During the project I will work on WP3 and develop analysis techniques to evaluate attack scenarios and countermeasures with respect to quantitative security properties. In my free time, I like to read books, spend time with friends and meet new people. I enjoy traveling and discovering new cultures.

Selected Publications

ADTool: Security Analysis with Attack–Defense Trees

Barbara Kordy, Piotr Kordy, Sjouke Mauw, Patrick Schweitzer

ADTool is free, open source software assisting graphical modeling and quantitative analysis of security using attack–defense trees. The main features of ADTool are easy creation, efficient editing, and automated bottom-up evaluation of security-relevant measures. The tool also supports the use of attack trees, protection trees and defense trees, which are all particular instances of attack–defense trees.

link.springer.com/chapter/10.1007%2F978-3-642-40196-1_15

New Efficient Utility Upper Bounds for the Fully Adaptive Model of Attack Trees

Ahto Buldas, Aleksandr Lenin

We present a new, fully adaptive computational model for attack trees that allows attackers to repeat atomic attacks if they fail and to play on if they are caught and have to pay penalties. The new model allows safer conclusions about the security of real-life systems and is somewhat (computationally) easier to analyze. We show that in the new model optimal strategies always exist and that finding the optimal strategy is (just) an np-complete problem. We also present methods to compute adversarial utility estimation and utility upper bound approximated estimation using a bottom-up approach.

link.springer.com/chapter/10.1007%2F978-3-319-02786-9_12

Time-Dependent Analysis of Attacks

Florian Arnold, Holger Hermanns, Reza Pulungan, Mariëlle Stoelinga

The success of a security attack crucially depends on time: the more time available to the attacker, the higher the probability of a successful attack; when given enough time, any system can be compromised. Insight into time-dependent behaviors of attacks and the evolution of the attacker’s success as time progresses is therefore a key for effective countermeasures in securing systems.

This paper presents an efficient technique to analyze attack times for an extension of the prominent formalism of attack trees. If each basic attack step, i.e., each leaf in an attack tree, is annotated with a probability distribution of the time needed for this step to be successful, we show how this information can be propagated to an analysis of the entire tree. In this way, we obtain the probability distribution for the entire system to be attacked successfully as time progresses. For our approach to be effective, we take great care to always work with the best possible compression of the representations of the probability distributions arising. This is achieved by an elegant calculus of acyclic phase type distributions, together with an effective compositional compression technique. We demonstrate the effectiveness of this approach on three case studies, exhibiting orders of magnitude of compression.

link.springer.com/chapter/10.1007%2F978-3-642-54792-8_16

RISK-DET: ICT Security Awareness Aspect Combining Education and Cognitive Sciences

Guillaume Schaff, Carlo Harpes, Matthieu Aubigny, Marianne Junber, Romain Martin

This paper explains the main innovation of a risk assessment tool, called RISK-DET, that includes an ICT risk awareness aspect supported by a specific application: Voozio 2.0. The design of the RISK-DET tool considers the implementation of the emergent ICT (Information and Communication Technology) Risk Detection Skill (IRDS) concept. Today, the users' inability to detect a risk situation is a real security problem and represents a societal challenge. According to the results of a security experiment based on a malicious smartphone application called Voozio 1.0, the main reason for this problem is the absence of effective ICT security awareness training programs adapted to users' needs. To prove and confirm this hypothesis, we aim to evolve the Voozio application in the 2.0 version. This new version will be able to determine the ability of ICT users to detect a risk situation and improve it by combining cognitive sciences and education technologies. In our paper, we will describe the specifications of the new version of Voozio. We also present the Voozio 2.0 implementation framework.

eprints.eemcs.utwente.nl/secure2/00024791/01/ART_007_itrust-Scientific_article_ICCGI_GSC_V2.2_gsc.pdf

Cost-Effectiveness of Security Measures: A Model-Based Framework

Wolter Pieters, Christian W. Probst, Zofia Lukszo, Lorena Montoya

Recently, cyber security has become an important topic on the agenda of many organisations. It is already widely acknowledged that attacks do happen, and decision makers face the problem of how to respond. As it is almost impossible to secure a complex system completely, it is important to have an adequate estimate of the effectiveness of security measures when making investment decisions. Risk concepts are known in principle, but estimating the effectiveness of countermeasure proves to be difficult and cannot be achieved by qualitative approaches only. In this chapter, the authors consider the question of how to guarantee cost-effectiveness of security measures. They investigate the possibility of using existing frameworks and tools, the challenges in a security context as opposed to a safety context, and directions for future research.

www.igi-global.com/chapter/cost-effectiveness-of-security-measures/94285

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.