Automating Security Risk Management and Threat Modeling

Olga Gadyatskaya

SnT, University of Luxembourg
olga.gadyatskaya@uni.lu

Thesis Details

Risk assessment (threat analysis) is traditionally performed by a group of human analysts (think consulting companies that charge per hour) by brainstorming about potential threats to the organization. This activity produces incomplete results, because humans are not able to take into account all possible scenarios [7]. Thus lately security researchers, including our group, started to work on automated risk assessment techniques, in which threats and potential attacks are identified automatically from some system model [2, 6, 8].

Risk management activity also includes risk treatment: identification of countermeasures that need to be introduced in the organization in order to reduce risks to acceptable levels. In this thesis you will make research in the general area of automated risk management with attack trees. Possible topics for a Master thesis are below.

Topic 1: Automated assignment of countermeasures into an attack tree

Assume that security analysts have designed an attack tree characterizing existing attacks for an organization. For such a tree there exist several approaches to identify the most critical attack scenarios (based on parameters important for the attacker, such as cost or time, or parameters important for the defender, such as impact). Given the set of the most severe attacks, we would like to automatically produce a set of countermeasures thwarting these attacks.

You will work on identifying a plausible approach for automated preventive security controls selection. This approach will likely require a knowledge base/an ontology that will capture applicable countermeasures for each attack type (we can start from, e.g., CAPEC). Given such a knowledge base, you will design an algorithm to select countermeasures based on some chosen metrics (e.g., risk leverage, impact reduction, likelihood reduction). You will also need to investigate how to accommodate the selected countermeasures in the original attack tree (thus yielding a correct attack-defence tree). The overall approach will be implemented as a prototype tool and integrated with the ADTool format [4].

A preliminary study for this topic has been published in [3]; this is a result of a previous successful Master project. The goal will be to extend this work with more sophisticated countermeasure selection approaches.

Details: 10% theoretical work (on the countermeasure selection metrics and the correctness of attack-defence tree checking); 60% practical research work; 30% programming is expected. This tentative balance can be further revised based on how the research will evolve.

Topic 2: Comparison of automatically generated attack trees versus manually designed

Recently several tools emerged that aim at automated construction of attack scenarios expressed as attack trees [2]. These tools however produce "flat trees", i.e., they do not structure the attack scenarios in some abstract way [6]. Human analysts instead aim at establishing categories of attacks, with more abstract attack steps appearing closer to the root of the tree [1]. In this thesis you will study existing methodologies for automated and manual design of attack trees, and will propose a taxonomy of attack tree properties that will bridge the gap between "flat" and "abstract" attack trees.

Details: 20% theoretical work (studying the existing attack tree semantics, including the refinement semantics from [6]); 60% practical research work (studying existing practical approaches and establishing the taxonomy) is expected. This tentative balance can be further revised based on how the research will evolve.

Topic 3: Sensitivity analysis on attack-defense trees

Assume that security analysts have designed a comprehensive attack-defense tree representing the existing attacks and already existing controls for an organization. Given this tree, quantitative analysis for various attributes (time, cost, probability of success, impact of an attack) can be performed in the ADTool [4]. *Sensitivity analysis* is a method for experimenting with different attribute values to identify critical paths in the tree. In the nutshell, the analyst tries to establish how variance in some attribute values affects the value for the root node.

The goal of this thesis will be to establish a methodology for sensitivity analysis on attack-defense trees. For example, if the analyst goal is to establish the place to introduce a new security control, what process does she need to follow? This methodology will be implemented as a prototype tool and integrated with the ADTool format.

Details: 60% design work; 40% programming is expected. This tentative balance can be further revised based on how the work will evolve.

Topic 4: Cyber-insurance propositions modeling with attack trees

Cyber-insurance is a recent solutions for many companies to share risks. These companies may rely on already available internal risk assessment results to understand the cost/benefit ratio of various cyber-insurance propositions.

The first goal of this thesis is to review the cyber-insurance products available in Luxembourg, and to relate them to attacks that can be expressed in attack trees (e.g., such as the tree developed for the ATM security in [1]). Then you will develop a methodology to assess costs and risk exposure for the insured and the insurer sides that will integrate insights from attack tree-based quantitative (e.g. like in [5]) and qualitative analyses.

Details: 30% theoretical work (studying attack tree semantics and analysis techniques); 70% practical research work is expected (studying cyber-insurance propositions and developing the methodology). This tentative balance can be further revised based on how the work will evolve.

References

1. Fraile, M., Ford, M., Gadyatskaya, O., Kumar, R., Stoellinga, M., Trujillo-Rasua, R.: Using attackdefense trees to analyze threats and countermeasures in an ATM: A case study. In: Proc. of PoEM. Springer (2016)
2. Gadyatskaya, O.: How to generate security cameras: Towards defence generation for socio-technical systems. In: Proc. of GraMSec. LNCS, vol. 9390, pp. 50–65. Springer (2015)
3. Gadyatskaya, O., Harpes, C., Mauw, S., Muller, C., Muller, S.: Bridging two worlds: Reconciling practical risk assessment methodologies with theory of attack trees. In: Proc. of GraMSec. Springer (2016)
4. Gadyatskaya, O., Jhawar, R., Kordy, P., Lounis, K., Mauw, S., Trujillo-Rasua, R.: Attack trees for practical security assessment: Ranking of attack scenarios with ADTool 2.0. In: Proc. of QEST. LNCS, vol. 9826, pp. 159–162. Springer (2016)
5. Gadyatskaya, O., Hansen, R.R., Larsen, K.G., Legay, A., Olesen, M.C., Poulsen, D.B.: Modelling attack-defense trees using timed automata. In: Proc. of FORMATS. pp. 35–50. Springer (2016)
6. Gadyatskaya, O., Jhawar, R., Mauw, S., Trujillo-Rasua, R., Willemse, T.A.: Refinement-aware generation of attack trees. In: Proc. of STM. pp. 164–179. Springer (2017)
7. Gadyatskaya, O., Labunets, K., Paci, F.: Towards empirical evaluation of automated risk assessment methods. In: Proc. of CRiSIS. pp. 77–86. Springer (2016)
8. Gadyatskaya, O., Trujillo-Rasua, R.: New directions in attack tree research: Catching up with industrial needs. In: Proc. of GramSec. pp. 115–126. Springer (2017)