State-based attack–defense trees

Barbara FILA and Sophie PINCHINAT

Master internship proposal for year 2020–2021
at *Institut de Recherche en Informatique et Systèmes Aléatoires* (IRISA),
Rennes, France

1 Context

Formal methods and tools are commonly used to support risk analysis and risk assessment activities [1]. Numerous graphical approaches to model and reason about systems' vulnerabilities and possible attacks exist. Among them attack trees are one of the most commonly used by industry [2]. An attack tree decomposes the ultimate goal of the attacker into simpler goals and actions that need to be performed to attack a system. Such a hierarchical decomposition is beneficial as it makes efficient quantitative analysis of security possible.

The classical attack tree model considers only the attacker's point of view, so it is insufficient to address the fundamental objective of the risk management, namely, identify countermeasures that could secure the analyzed system, in such a way that the residual risks are acceptable. To overcome this problem, attack trees have been extended with the nodes representing countermeasures. The resulting formalism is called attack–defense trees [3]. Roughly speaking, an attack–defense tree can be seen as a game between an attacker trying to attack the system and a defender trying to protect it.

2 Scientific challenge

In the context of attack tree-based models, the main scientific challenge is to develop their formal foundations including clear semantics as well as algorithms supporting their manipulation. It is beneficial because the creation and analysis of well-formalized models can be automated in thus becomes scalable.

Two approaches to formalize attack trees exist: the older one is based on actions, and the more recent one on states. The action-based approach is concerned with actions or objectives to be reached by the attacker and which are represented by the attack tree nodes [4]. The state-based approach makes a link between the attacker's goals and the states of the analyzed system explicit [5, 6]. In this second approach, the attacks are sequences of the system states. Although not yet sufficiently studied, the state-based approach is very promising, as it allows to address new questions regarding the quality and the suitability of an attack tree for the analyzed system. It can also take advantage of a vast body of formal verification techniques and tools supporting transition systems theory.

3 Objective

Current foundations of attack–defense trees are all based on actions [7, 8, 9]. The objective of this internship is to combine the power of the extended attack–defense tree modeling with the power of the state-based formalization. In other words, our goal is to develop a state-based semantics for attack–defense trees in the presence of a formal model – a labeled transition system – of the analyzed system. The implications of such a formalization are numerous: if the system model captures relevant environmental elements, the scope of the attack–defense tree analysis can be extended to accidental events in addition to the malicious ones; the quality of an attack–defense tree wrt the analyzed system can be evaluated; a clear difference between preventive and reactive countermeasures in attack–defense trees becomes possible; and finally, the ATSyRA tool[1] supporting attack tree creation and analysis, and developed in collaboration with the French ministry of defense (DGA-MI), can be extended to attack–defense trees.

[1] `http://atsyra2.irisa.fr/`

4 Supervisors and research environment

This internship will be supervised by prof. Sophie Pinchinat and dr Barbara Fila from IRISA, Rennes in France. Sophie Pinchinat[2] is an expert in logic and multi-agents systems. She introduced the state-based model for attack trees and is the main creator of the ATSyRA tool. She is the head of the LogicA[3] (*Logic and Applications*) team at IRISA. Barbara Fila[4] (previously Kordy) is one of the inventors of the attack–defense tree model and works mainly on quantitative security analysis using graphical modeling. She is member of the EMSEC[5] (*Embedded Security and Cryptography*) team at IRISA.

The internship will take place at IRISA[6] in Rennes, France. IRISA is today the largest French research laboratory (850+ people) in the field of computer science and information technology. The lab covers all the themes within these fields, from computer and network architecture to artificial intelligence, going through, e.g., security, software engineering, distributed systems and virtual reality.

It is a five month master internship, paid according to the official French rules (*gratification de stage classique*). We foresee to have an opening for a Ph.D. position in autumn 2021 (funding to be confirmed), to continue the research initiated in this project.

5 Contact and applications

For all inquiries please contact Barbara Fila (`barbara.fila@irisa.fr`) *and* Sophie Pinchinat (`sophie.pinchinat@irisa.fr`). Informal inquiries are welcome.

To apply, please send us your CV and the grade transcript of all university-level courses taken.

References

[1] Wojciech Wideł, Maxime Audinot, Barbara Fila, and Sophie Pinchinat. Beyond 2014: Formal methods for attack tree-based security modeling. *ACM Comput. Surv.*, 52(4):75:1–75:36, 2019.

[2] Bruce Schneier. Attack Trees: Modeling Security Threats. *Dr. Dobb's Journal of Software Tools*, 24(12):21–29, 1999.

[3] Barbara Kordy, Sjouke Mauw, Sasa Radomirovic, and Patrick Schweitzer. Attack–defense trees. *J. Log. Comput.*, 24(1):55–87, 2014.

[4] Sjouke Mauw and Martijn Oostdijk. Foundations of attack trees. In *ICISC*, volume 3935 of *Lecture Notes in Computer Science*, pages 186–198. Springer, 2005.

[5] Maxime Audinot, Sophie Pinchinat, and Barbara Kordy. Is my attack tree correct? In *ESORICS (1)*, volume 10492 of *Lecture Notes in Computer Science*, pages 83–102. Springer, 2017.

[6] Maxime Audinot, Sophie Pinchinat, and Barbara Kordy. Guided design of attack trees: A system-based approach. In *CSF*, pages 61–75. IEEE Computer Society, 2018.

[7] Barbara Kordy and Wojciech Wideł. On quantitative analysis of attack–defense trees with repeated labels. In *POST*, volume 10804 of *Lecture Notes in Computer Science*, pages 325–346. Springer, 2018.

[8] Barbara Fila and Wojciech Wideł. Efficient attack–defense tree analysis using pareto attribute domains. In *CSF*, pages 200–215. IEEE, 2019.

[9] Barbara Fila and Wojciech Wideł. Exploiting attack–defense trees to find an optimal set of countermeasures. In *CSF*, pages 395–410. IEEE, 2020.

[2] `http://people.irisa.fr/Sophie.Pinchinat/`
[3] `http://www-logica.irisa.fr/`
[4] `http://people.irisa.fr/Barbara.Kordy/`
[5] `https://www.irisa.fr/emsec/`
[6] `https://www.irisa.fr/en`