Attack–defense trees for real life applications

Sjouke Mauw, Stéphane Paul, Barbara Kordy, Piotr Kordy

Joint master project between the University of Luxembourg and Thales Research & Technology France

Background

Attack–defense trees (ADTrees) [5] extend the well known model of attack trees [10, 9] with the possibility of modeling not only the attacker's actions but also countermeasures of the defender of a system.

A lot of research has been performed concerning formal specification and semantics for ADTrees during last three years [4, 7, 6, 3, 2]. A description of a realistic case study using the ADTree methodology for analysis of RFID security can be found in [1]. Furthermore, a computer tool, called the ADTool, supporting creation, modular display and quantitative analysis of ADTrees has been implemented [8] as part of the national research project ATREES [2].

Objectives

The main goal of the current master project is to validate the ADTree methodology on a real-life case study and to extend it further in order to make it suitable for risk assessment of large industrial security scenarios.

The main steps of the master project will be

1. **Selection of the application domain.** A case study of interest for all involved parties will be selected jointly by the student, the company and the university. The case study itself is not the main objective of this project. The case study is meant to guide the research to be performed in the project, in particular to
   - identify relevant requirements and assumptions,
   - understand industrial needs related to graphical security modeling,
   - illustrate developed concepts and proposed solutions.

2. **Analysis.** The ADTree methodology will be used for analysis of the identified case study. This step will be composed of the following tasks:

   - development of ADTree models depicting attack–defense scenarios relevant for the identified application domain;
   - development of re-usable attack and defense patterns related to the proposed scenarios;
   - ranking of possible attacks and proposed countermeasures based on quantitative analysis of developed models.

   In this step of the project the current ADTree methodology will be validated on a large scenario. This will lead to the identification of the drawbacks and insufficiencies of the current framework with respect to modeling and analysis of large industrial cases.

3. **Extension of the ADTree methodology.** The main objective of the project will be to extend the current ADTree methodology and propose solutions for insufficiencies identified in the previous step. The following actions are foreseen:

   - development of methods for better scalability of the ADTree models and their maintainability for long-lived systems;
   - identification of new attributes, especially relevant for assessing risk in real-life applications;
   - integration of the standard XML format representation of trees into the current ADTree methodology;
   - implementation of the proposed extensions in the ADTool;
   - assessment of the efficiency and scalability of the proposed approach.

Contact

For all inquiries about the project, please contact Dr. Barbara Kordy at `barbara.kordy@uni.lu`

References

[1] Alessandra Bagnato, Barbara Kordy, Per Håkon Meland, and Patrick Schweitzer. Attribute Decoration of Attack–Defense Trees. *International Journal of Secure Software Engineering (IJSSE)*, 3(2):1–35, 2012.

[2] Barbara Kordy, Piotr Kordy, Sjouke Mauw, Saša Radomirović, Patrick Schweitzer, and Jean-Paul Weber. The ATREES Project, funded by the Fonds National de la Recherche, Luxembourg under grants C08/IS/26 and PHD-09-167. `http://satoss.uni.lu/projects/atrees/`, 2009–2012. Accessed October 12, 2012.

[3] Barbara Kordy, Sjouke Mauw, Matthijs Melissen, and Patrick Schweitzer. Attack–Defense Trees and Two-Player Binary Zero-Sum Extensive Form Games Are Equivalent. In Tansu Alpcan, Levente Buttyán, and John S. Baras, editors, *GameSec*, volume 6442 of *LNCS*, pages 245–256. Springer, November 2010.

[4] Barbara Kordy, Sjouke Mauw, Saša Radomirović, and Patrick Schweitzer. Foundations of Attack–Defense Trees. In Pierpaolo Degano, Sandro Etalle, and Joshua D. Guttman, editors, *FAST*, volume 6561 of *LNCS*, pages 80–95. Springer, September 2010.

[5] Barbara Kordy, Sjouke Mauw, Saša Radomirović, and Patrick Schweitzer. Attack–Defense Trees. *Journal of Logic and Computation*, pages 1–33, 2012. available online `http://logcom.oxfordjournals.org/content/early/2012/06/21/logcom.exs029.short?rss=1`.

[6] Barbara Kordy, Sjouke Mauw, and Patrick Schweitzer. Quantitative Questions on Attack–Defense Trees. *arXiv*, 2012. Available at `http://arxiv.org/abs/1210.8092`.

[7] Barbara Kordy, Marc Pouly, and Patrick Schweitzer. Computational Aspects of Attack–Defense Trees. In *Security & Intelligent Information Systems*, volume 7053 of *LNCS*, pages 103–116. Springer, 2011.

[8] Piotr Kordy and Patrick Schweitzer. The ADTool. `http://satoss.uni.lu/members/piotr/adtool/index.php`, 2012. Accessed October 12, 2012.

[9] Sjouke Mauw and Martijn Oostdijk. Foundations of Attack Trees. In Dongho Won and Seungjoo Kim, editors, *ICISC*, volume 3935 of *LNCS*, pages 186–198. Springer, 2005.

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