Modelling of Attack Trees for Security Assement of Hardening Mechanisms

Bachelor's Thesis

Supervisor: Prof. Dr. Alexander Pretschner
Advisor: Patrick Stöckle
Email: {alexander.pretschner, patrick.stoeckle}@tum.de
Phone: +49 (89) 289 - 17314
Starting date: immediately

Fakultät für Informatik
Lehrstuhl 4
Software & Systems Engineering
Prof. Dr. Alexander Pretschner

Boltzmannstraße 3
85748 Garching bei München

Tel: +49 (89) 289 - 17314
https://www4.in.tum.de

Context

Attack trees [4] are conceptual diagrams showing how an asset, or target, might be attacked. In the field of information technology, they have been used to describe threats on computer systems and possible attacks to realize those threats. Currently, we at the Chair of Software and Systems Engineering (I4) in cooperation with an industry partner are developing the Scapolite hardening-framework. The goal of Scapolite is the automatic extraction, validation, and application of hardening mechanisms to make computer systems more secure. One part of Scapolite is the automatic assessment, which configuration decision on the system are currently set to which value. The problem is that usually one configuration decision alone does not allow or deny an attack, but only the combination of several of them. Here, the attack trees should be applied by expressing the relation ship between different configuration decisions. The idea of this Bachelor's thesis is to combine the hardening mechanisms of Scapolite with the assessment capabilities of attack trees.

Goal

The goal of this thesis is to develop a way to create and manage attack trees which can be combined with the results of an Scapolite assessment to evaluate which attack is currently possible and which is not. If the method to create and manage the attack has to be created from scratch or if existing tools, e.g., [3], can be adjusted has to be investigated. The method to model the attack trees should be based on an EMF model. One should be able to model the attack tree through a textual syntax, e.g., based on Xtext [1], and optional through a graphical syntax, e.g., based on Sirius [2]. In the end, the method should be evaluated using a set of attack trees combined with results from the Scapolite assessment process.

Working Plan

1. Familiarize with attack trees
2. Familiarize with Scapolite
3. Create a new model for attack trees or adjust a existing
4. Create the textual syntax
5. Create the graphical syntax
6. Develop and implement the algorithm how to examine which attacks are possible and which are not.
7. Evaluate

References

[1] . URL https://www.eclipse.org/Xtext/.

[2] . URL https://www.eclipse.org/sirius/.

[3] Rajesh Kumar, Stefano Schivo, Enno Ruijters, Buğra Mehmet Yildiz, David Huistra, Jacco Brandt, Arend Rensink, and Mariëlle Stoelinga. Effective analysis of attack trees: A model-driven approach. Fundamental Approaches to Software Engineering, pages 56–73. Springer International Publishing. ISBN 978-3-319-89363-1.

[4] Sjouke Mauw and Martijn Oostdijk. Foundations of attack trees. Information Security and Cryptology - ICISC 2005, pages 186–198. Springer Berlin Heidelberg. ISBN 978-3-540-33355-5.