Graphical Specification Language for the Entity-Labeling Aspect

Exposé – Master Thesis

Philipp Schwetschenau
Ilmenau University of Technology
philipp.schwetschenau@tu-ilmenau.de

May 15, 2018

1 Introduction

With the increasing number of IT systems, securing these systems became an obvious and important issue. For this purpose many security models and model families were developed for a wide field of application over the last years.

Because quantity and variety of these models grow just as much as their relevance for security-critical applications the model-based security engineering process became more complex and therefore error-prone to human deviations. Formal security models may offer possibilities to analyze them concerning security properties, but also new sources of errors may be introduced due to their high abstraction level in the process of engineering them.

[Amt18] proposed a new approach called Aspect-oriented Security Engineering (AOSE) which claims to close semantic gaps between steps in the security engineering process (requirements, informal policy, formal model) to reduce the potential impact of human errors. This approach roughly adapts the idea of the aspect-oriented programming paradigm. It tailors all steps to aspects, which are non-functional requirements of the engineering process like determining requirements of policy semantics or analyzing certain security goals. There are two major classes for aspects regarding AOSE: related to policy analysis and to policy semantics.

One possible aspect of the latter is the Entity Labeling Aspect (EL). It is designed to formally specify policy semantics typically found in operating systems and middleware systems. Therefore it bridges the gap and supports the transformation between informal policy and formal model. EL classifies model components into six semantic categories. These categories are typed as sets, assignments, rules or constraints. Interrelations between set-based categories are described by other categories to determine the policy's semantics. The notation is on a mathematical basis.

2 Motivation

The goal of reducing the impact of human errors by closing semantic gaps as much as possible with the help of AOSE/EL requires handling another formal notation, which is,

in this case, EL itself and its classification into the six semantic categories. To support working with this approach a graphical representation seems to be helpful to support and enhance the transition between informal and formalized notation. Especially this supports communication between different groups of people involved like model engineers, security architects, software developers, future administrators and clients, who have to cooperate and coordinate and all have different levels of experience regarding this topic.

[Amt18] already uses visual representations to illustrate examples. However, the representations are not described in detail as well as they seem to be inconsistent and ambiguous regarding several parts of the formalization (e.g. arrows can have several meanings and there is no way to specify functions with multiple input parameters). So these visualizations seem appropriate to underline and roughly visualize an already formalized policy after EL-based model engineering, but are not suitable for independent modeling on a stand-alone level, because they are not equivalent to their formalized mathematical counterpart.

There are two types of visualization [Amt18] used, which have different levels of abstraction: One is based on the actual model components and visualizes them and their relationships. The other one is based on a higher level of abstraction and visualizes the EL with its structure of semantic categories and their relationships.

Eventually to be able to independently and visually model and work on EL-based policies there is need for an unambiguous formal graphical specification language.

3 Goal

The main goal is to develop a graphical specification language for EL-based security polices. This should focus on clean and unambiguous semantics of the language.

The use of the language should be as simple as possible and as comprehensive as needed. Therefore its appearance and elements should be clear and well-structured. A selection of appropriate symbols and geometrical shapes for their equivalent model counterparts has to be made regarding an intuitive understanding and workflow. This selection should not be designed contradictory or conflicting to already established notations, especially those, which may be used in the context of security engineering.

It should be evaluated how feasible and reasonable it is to develop equivalent counterparts for every possible element and relationship in context of EL and to display all of them at once. This may also lead to the question how the visualization is related to a visualization on a higher abstraction level and how they are connected and might be managed. The latter may be investigated as an optional goal.

In addition to that a GUI-based editor should be developed as an prototype to make use of the proposed graphical specification language.

4 Solution

Based on cognitive psychology like gestalt laws and human optical perception on the one hand and based on usability and common best practices on the other hand, a graphical specification language should be developed. For this already existing and established visual notations like UML or ERD should be analyzed regarding their way of visualizing

structures and relationships for similar problems. This may lead to adopting ideas of those or at least get inspired by them.

A starting point could be the study and evaluation of the visual notation used by [Amt18]. This should give hints on what might be missing, what might be ambiguous and what are potential requirements for a new graphical specification language.

The development as well as the evaluation of the language should be supported by examples with different scope and complexity.

References

[Amt18] Peter Amthor. *An Aspect-oriented Approach to Model-based Security Engineering.* dissertation, Technische Universität Ilmenau, 2018.