Threat & Risk Information Sharing and Federation

Attack/Defense Tree Use-Case & Scenario

# Background and context

Attack and defense trees represent a proven methodology for describing and analizing risk scenarios. We build on the “Attack-Defense Tree”[[1]](#footnote-1) work of Patrick Schweitzer and utilize the “Attack–Defense Tree Methodology for Security Assessment”[[2]](#footnote-2) scenario and example by Barbara Kordy. This work expands the concept of “attack trees” with nodes for defense.

The example provided by Ms. Kordy is represented as instances of the threat/risk model. This model is then augmented with additional relationships made possible by threat/risk. This shows that the threat/risk model provides a basis for representing attack/defense trees in context.

# Reference Example

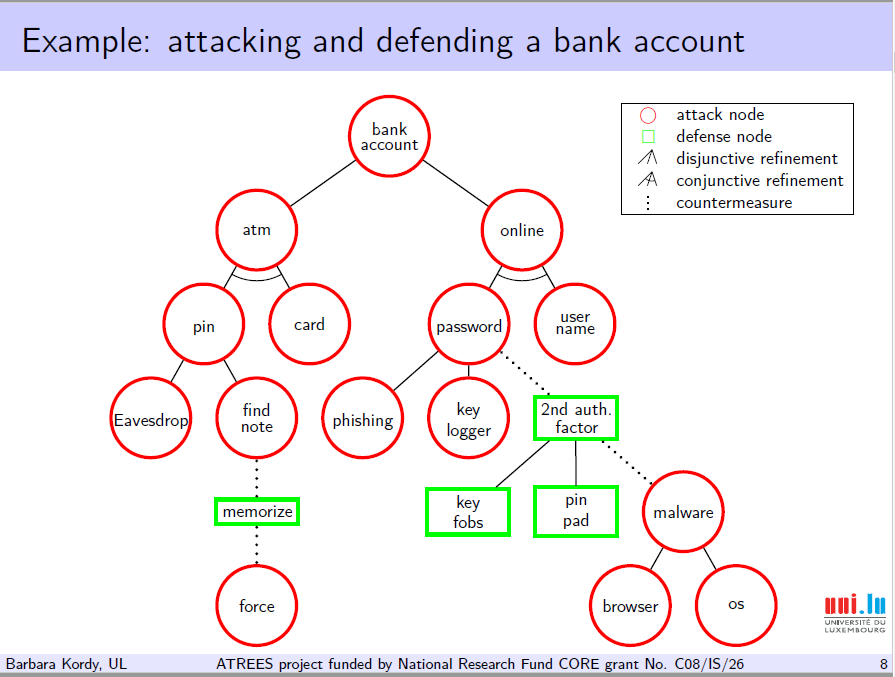


Figure 1Reference Example - bank account attack/defense tree

The above example shows the paths of attach and defense for a bank account via on-line and ATM access. Readers are directed to the referenced document for detail.

# Threat/risk scenarios

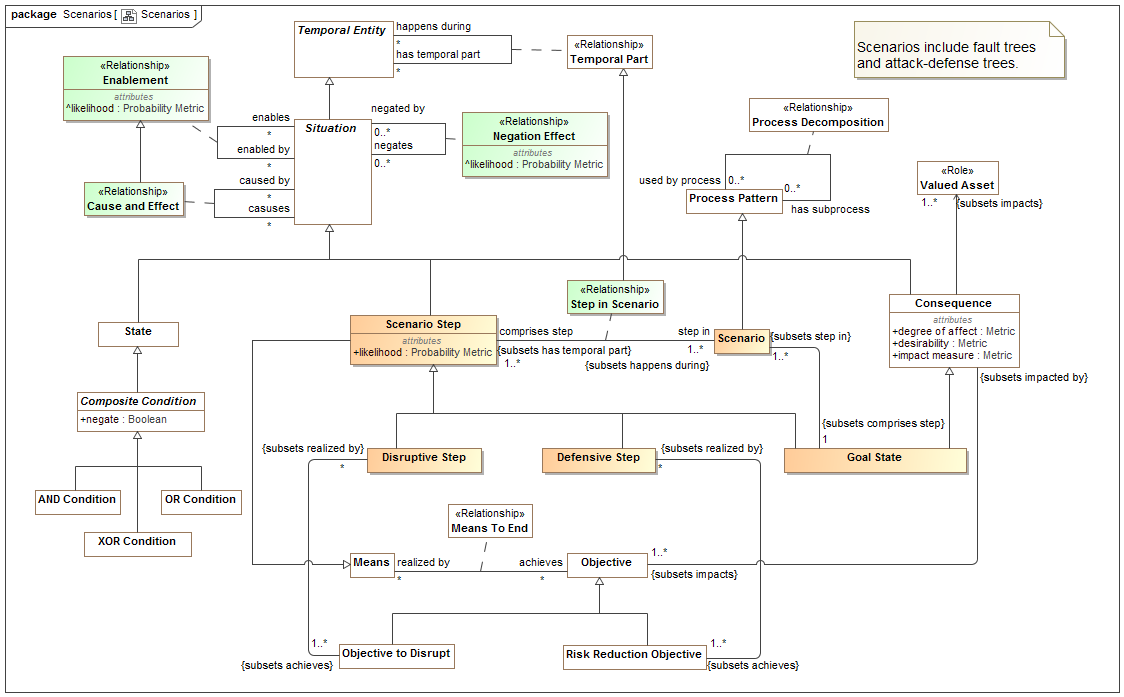


Figure 2Scenario package of the threat/risk model

The above diagram shows the “scenario” modeling package of the threat/risk model. Each “node” in an attack, defense or fault tree is a “Scenario Step” –those steps may be categorized as a goal state, disruptive or defensive. Enablement, cause & effect and negation relationships provide for the refinement of those steps.

# Threat/risk model instances

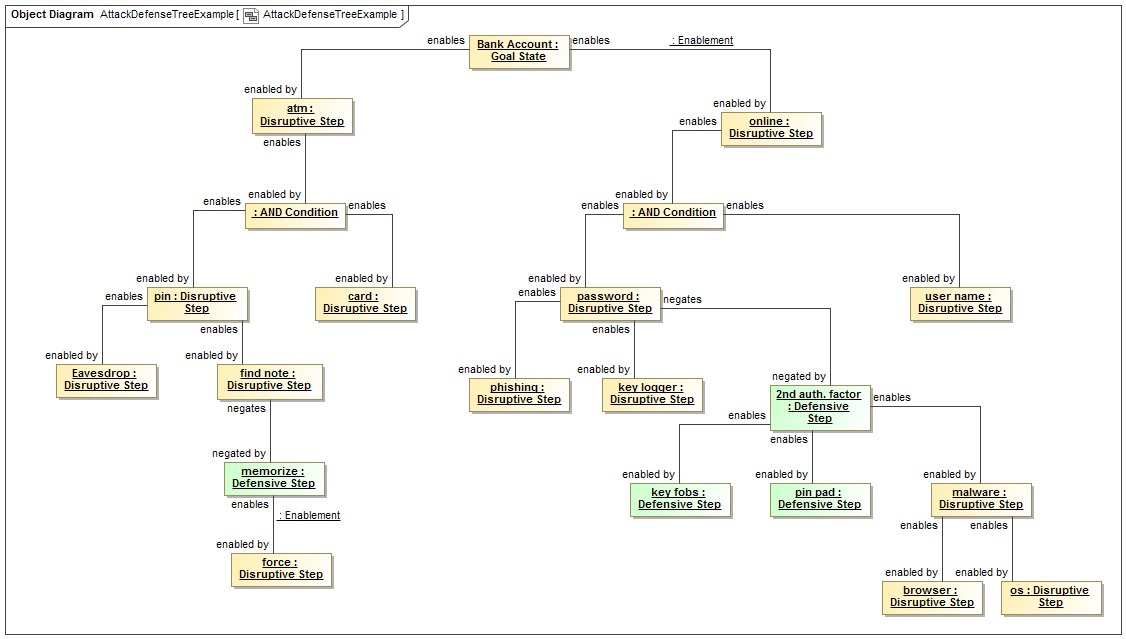


Figure 3Example as instances of a threat/risk model scenario

The above diagram shows instances of the threat/risk model that directly correspond to the nodes and relationships of the bank example. The “refinement” lines of the example are shown as instances of an “Enablement” relationship between the nodes where each node is a kind of situation.

# Additional threat/risk model instances

In addition to the relationships directly visible on an attack/defense diagram, additional information may be related to each step, including goals and stakeholders. Each step is considered part of a scenario.

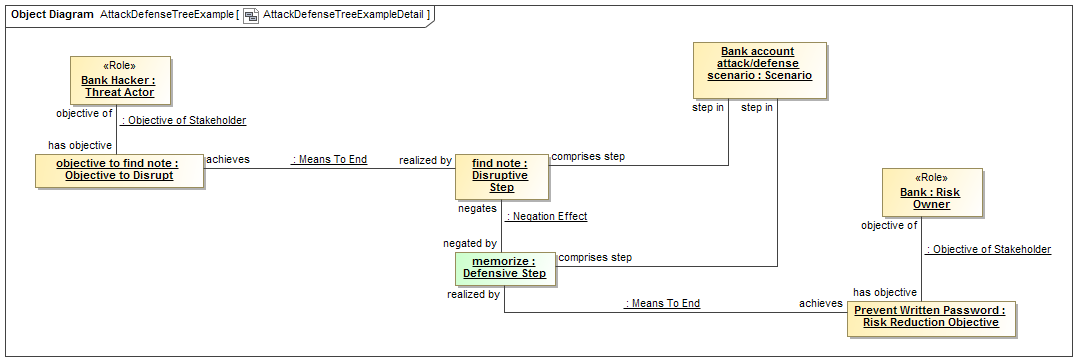


Figure 4 Additional scenario relationships

The above diagram shows some of the additional relationships that would enhance the operational picture. These include the owning scenario, objectives and stakeholders. Only two of the steps are shown at this level of detail to reduce diagram complexity.

# Conclusion

The above demonstrates that the threat/risk model is able to represent attack & defense trees as proposed by Schweitzer. The same scenario based capabilities may be used for other trees, such as fault trees. Integrating attack, defense and fault trees into the comprehensive threat/risk model enables better sharing, federation and analysis of complex and interrelated threat and risk information sources.

1. http://satoss.uni.lu/members/phd-theses/pschweitzer13-thesis.pdf [↑](#footnote-ref-1)
2. http://satoss.uni.lu/members/barbara/papers/slides.pdf [↑](#footnote-ref-2)