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 analyzing 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

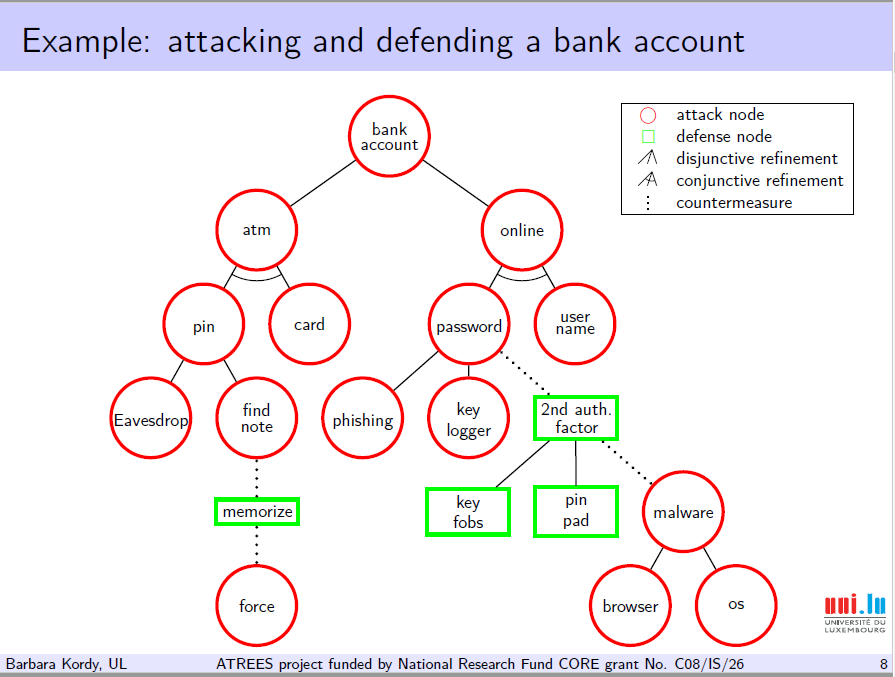


Figure Reference Example - bank account attack/defense tree

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

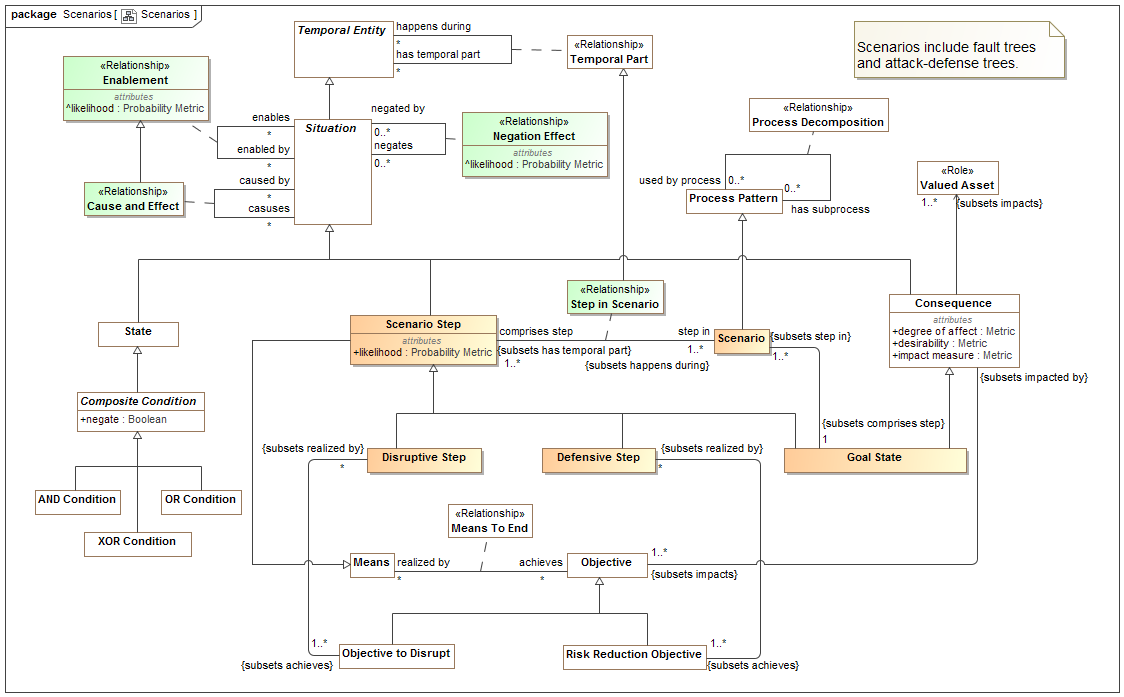


Figure Scenario package of the threat/risk model

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

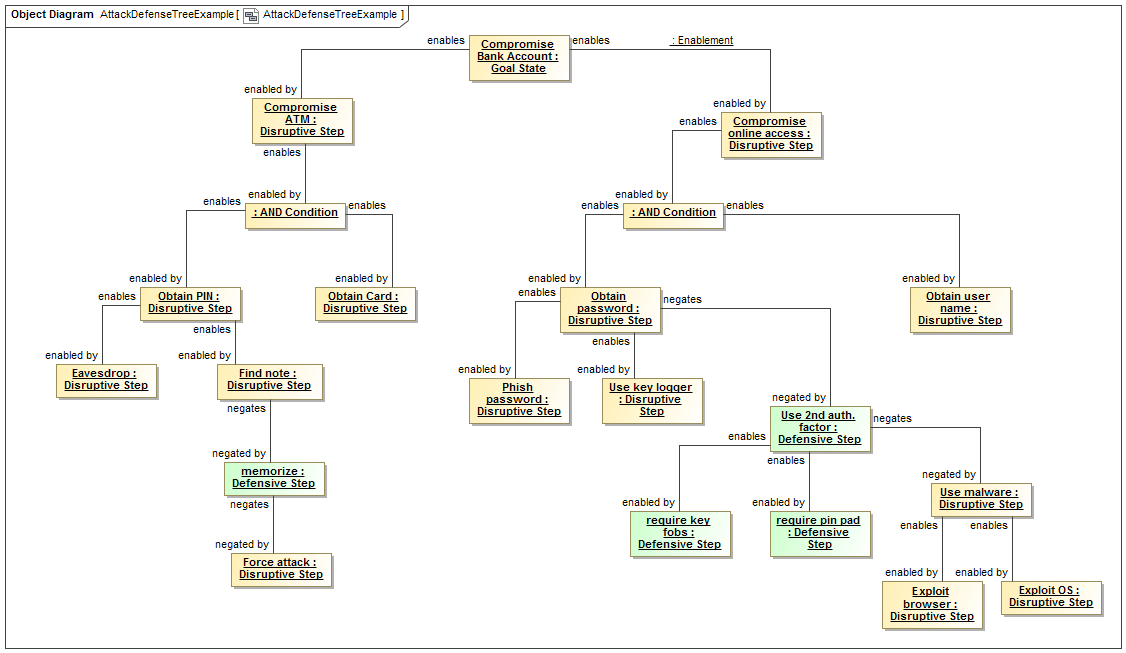


Figure Example as instances of a threat/risk model scenario

The above diagram shows instances of the threat/risk model that directly correspond to the nodes and relationships of the bank example. As each step (node) represents a desired action or state the abbreviated terms used in the example are augmented to make each a verb phrase for greater clarity (e.g. “atm” in the source example named “Compromise ATM” in the model).

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. This means that the “enabled by” step “enables” the next step. Alternatively, a defensive step (e.g. countermeasure) may “negate” a disruptive step, however a disruptive step may negate a defensive step, rendering it ineffective.

# 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.

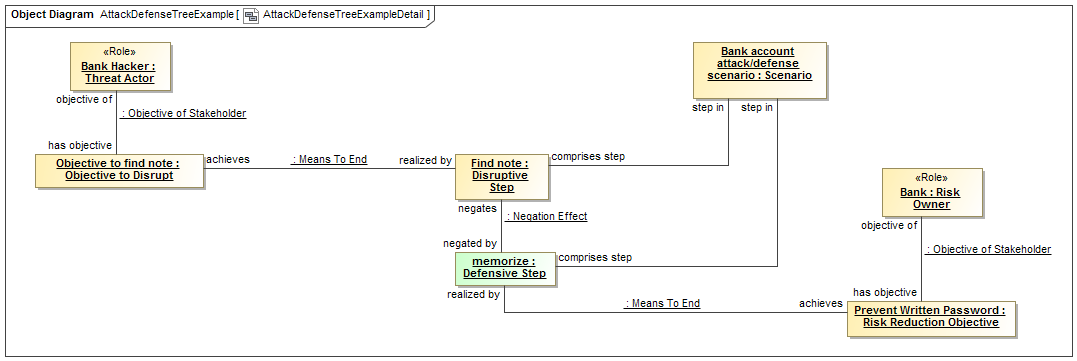


Figure Additional scenario relationships

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.

# Considering probabilities – source information

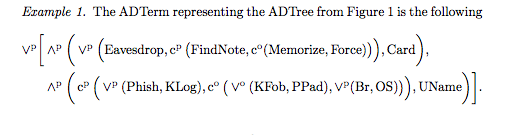
Attack trees become “computable” when probabilities and likelihoods are added. The following is based on Irisa[[3]](#footnote-3).

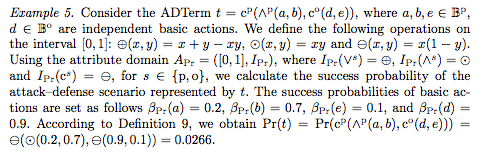
# Attack Defense Tree Probability Matrix

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Nodes** | **Type** | **Probability of Success** | **Probability of Success**  **as Function** | **Resource/Cost** | **Penalty of Failure** | **Threat/Defense Capability** | **Likelihood of Initiation** |
| Eavesdrop PIN | Attack | 0.5 |  |  |  |  |  |
| Find Note with PIN | Attack | 0.7 |  |  |  |  |  |
| Policy to Memorize | Defense | 0.9 |  |  |  |  |  |
| Brute Force to Find PIN | Attack | 0.2 |  |  |  |  |  |
| Steal the ATM Card | Attack | 0.2 |  |  |  |  |  |
| Phishing Password | Attack | 0.2 |  |  |  |  |  |
| Stealing Password Using KeyLogger | Attack | 0.05 |  |  |  |  |  |
| Use Key Fobs for Additional Authentication | Defense | 0.9 |  |  |  |  |  |
| Use PIN Pad for Additional Authentication | Defense | 0.9 |  |  |  |  |  |
| Bypass Multi-factor Authentication using Malware through the OS | Attack | 0.2 |  |  |  |  |  |
| Bypass Multi-factor Authentication using Malware through the Browser | Browser | 0.2 |  |  |  |  |  |
| Find Username | Attack | 0.7 |  |  |  |  |  |

The probably of successfully compromising the bank account can be computed using Example 1 in page 6, and Example 5 in page 13 Section 4.1 Bottom-up evaluation:

[**Foundations of Attack–Defense Trees - Irisa**](https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0ahUKEwjDxsao2cnSAhUHrVQKHVpNBUMQFggcMAA&url=http%3A%2F%2Fpeople.irisa.fr%2FBarbara.Kordy%2Fpapers%2Fadt.pdf&usg=AFQjCNEUl0yzD4eswblYo6jddAIx_eiU-w&sig2=fIvxwhdmotIr19mtnAR4Kw)





Using the above model, below probability of successful compromise is calculated.

The probability of succeeding ATM compromise is 12%.

The probability of succeeding online compromise is 4.3% with Multi-factor authentication.  Without it, the success rate of on-line attack is 13.6%.

If the attacker initiates attack on both avenues, the probability of successful compromise through both channels are 15.7%.

Without the multi-factor authentication, the success rate will be 24%

# Modeling probabilities

The above matrix proposes two scenarios – with and without multi-factor authentication. Each of these scenarios is modeled by adding asserted and computed likelihoods to each node in the tree. Each scenario is shown with a separate diagram.

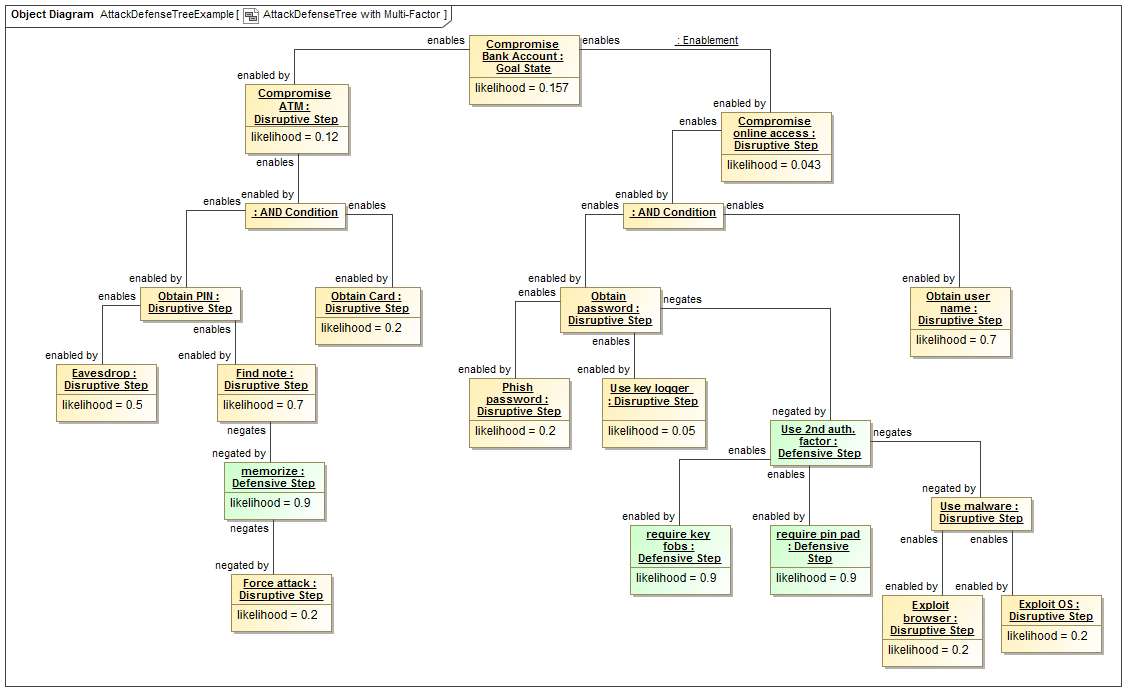


Figure Attack tree with asserted and computed likelihood added.

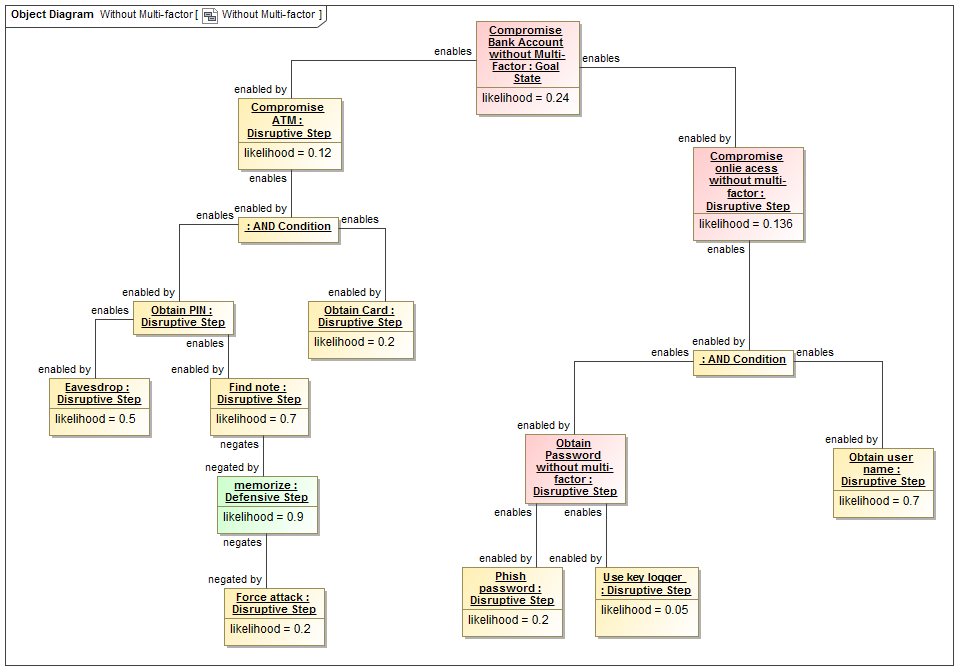


Figure Attack tree scenario without multi-factor

# Conclusion

The above demonstrates that the threat/risk model is able to represent attack & defense trees as proposed by Schweitzer. Processing the probability tree requires that each step (and optionally each enabling relationship) be assigned a likelihood. Computation of derivative likelihood is supported by the information provided but the algorithms for combining probabilities are not part of the standard.

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)
3. http://people.irisa.fr/Barbara.Kordy/papers/adt.pdf [↑](#footnote-ref-3)