Managing Security Risks Using Attack-Defense Tree

Presented by: Salman Lashkarara
Supervised by: Raimundas Matulevicius
University of Tartu, Institute of Computer Science, Software engineering curriculum

UNIVERSITY OF TARTU
Institute of Computer Science

Study IT in .ee
sponsored by Skype™

Project Idea

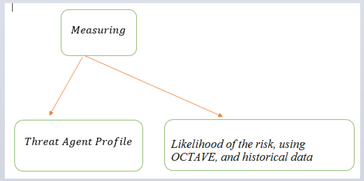
Current Attack-Defense Tree Problems [1]

- Does not consider Assets
- Does not distinguish between the attackers
- Does not point to the vulnerabilities which are exploited
- Uncertainty of a risk is not evaluated
- Effect of countermeasure is not evaluated
- Countermeasures are not comparable based on effectiveness, or cost

Alignment

Capabilities	***ADTree***	***Aligned ADTree***
Top-Down risk description	Supported	Supported
Top-Down countermeasure description	Supported	Supported
Managing vulnerabilities	Not Supported	Supported
Managing assets	Not Supported	Supported
Compare efficiency of countermeasures	Not Supported	Supported
Evaluate likelihood of the risk	Not Supported	Supported
Distinguish between threat agents	Not Supported	Supported

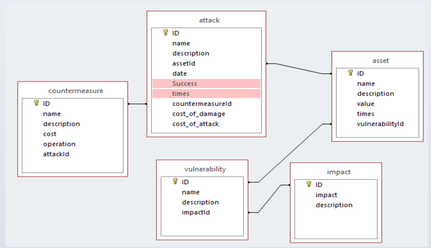
Measurement



Measurement

Evaluation of Probability of Risk Using OCTAVE[2] and Historical Data

Qualitative value	Definition	Quantitative value
Very High	More than 16 times in last 5 years	90%
High	6 - 15 times in last 5 years	70%
Medium	Five times in last 5 years	50%
Low	Three or four times in the last 5 years	20%
Very Low	Zero, one or two times in the last 5 years	10%



Given that the ***Asset*** was targeted, the probability of ***Attack*** is calculated as below:

$$P(Attack|Asset) = \frac{P(Asset \cap Attack)}{P(Asset)}$$

Threat Agent Profile

	Means				
	Computer means	People as asset	Process as assets	Intangible assets	Stepstone assets
Score	5	5	5	5	5

	Opportunities (Number of trial tries)			
	Zero	One	Finite	Infinite
Score	0	1	4	10

	Capabilities			
	Beginner	Undergraduate	Master	Specialist
Score	1	4	7	10

Measurement

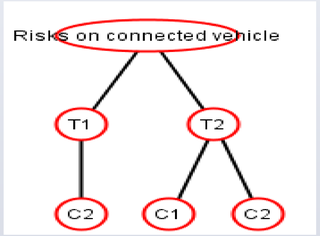
Threat Agent Profile

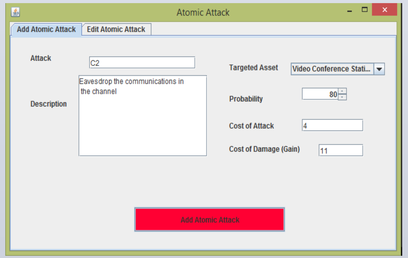
	Motivation					
	Curiosity	Personal fame	Personal Gain	Revenge	National interest	Ideology
Score	1	3	5	7	9	11

Evaluation of Threat Agent

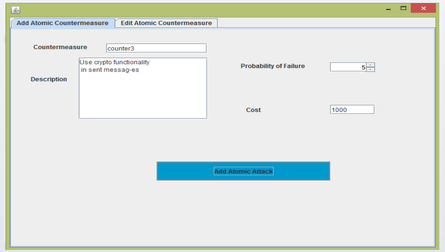
- ***score***= (Capability + Means + Motivation)*opportunity/4
- ***coefficient*** = score/115
- 115 is the maximum score of threat agent
- Likelihood considering threat agent = $P(Attack|Asset) *$ coefficient

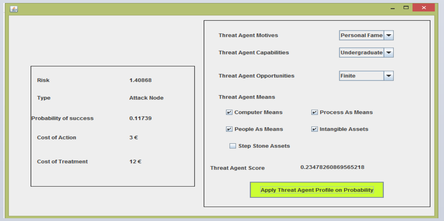
Implementation



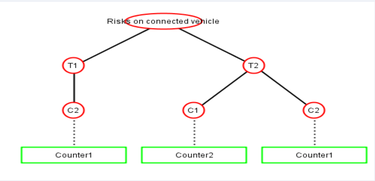


Implementation





Implementation



References

[1] Kordy, B. Kordy, P. Mauw, S. Schweitzer, P: ADTool: Security Analysis with Attack-Defense Trees (Extended Version), white paper, Accessed on: 19 Aguste 2016 on: https://www.researchgate.net/publication/236955204_ADTool_Security_Analysis_with_Attack-Defense_Trees_Extended_Version

[2] http://www.informit.com/articles/article.aspx?p=28469&seqNum=6

Website

https://github.com/salman-/A-ADTree/wiki