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

Project Idea
Current Attack-Defense Tree Problems

- 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

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

<table>
<thead>
<tr>
<th>Threat Agent Profile</th>
<th>Evaluation of Threat Agent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Score: 1</td>
<td>Score: 3</td>
</tr>
<tr>
<td>Capability</td>
<td>Means</td>
</tr>
<tr>
<td>Score: 1</td>
<td>Score: 4</td>
</tr>
<tr>
<td>100%</td>
<td>50%</td>
</tr>
</tbody>
</table>

Implementation
Website
https://github.com/salman-ADTree/wiki

References


Score
1 3 5 7 9 11

Opportunities
Zero One Finite Infinite

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

Score
5 5 5 5 5

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

Printed by...
www.PosterPresentations.com