New Directions in Attack Tree Research:

Catching up with Industrial Needs

Olga Gadyatskaya and Rolando Trujillo-Rasua

predict
prioritise
prevent
TRESPASS

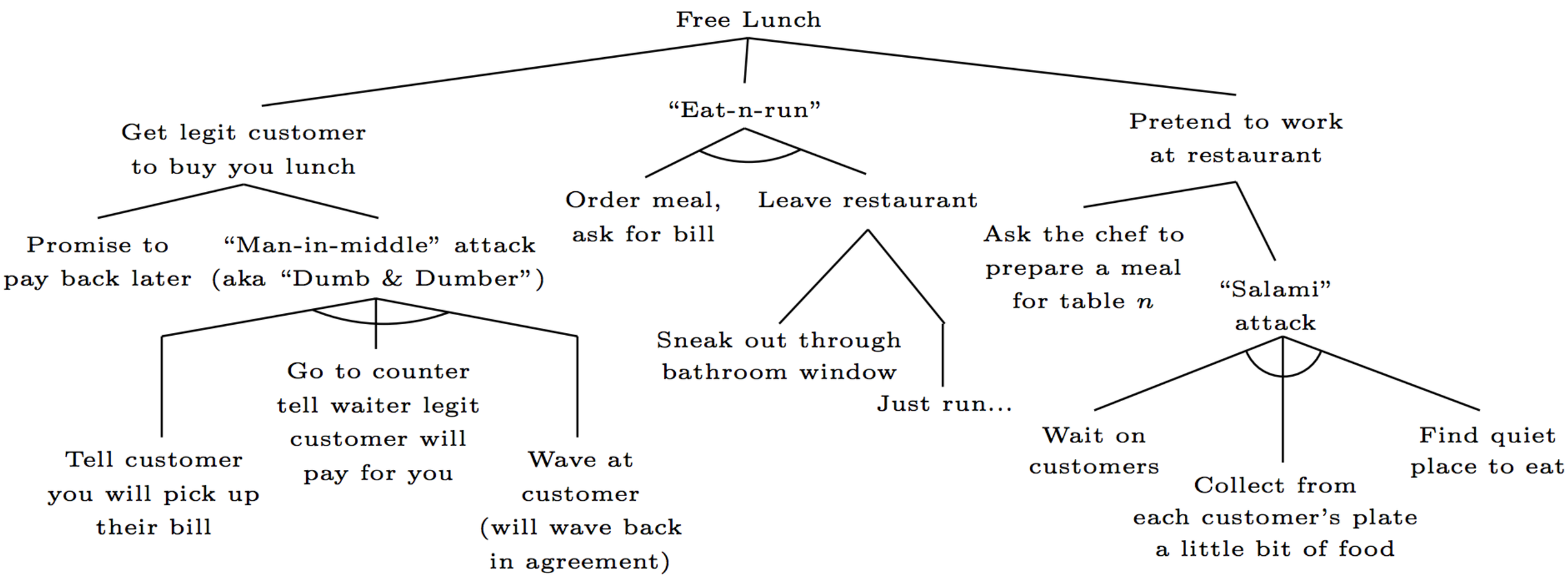
UNIVERSITÉ DU LUXEMBOURG

Fonds National de la Recherche Luxembourg

Attack trees

- Graphical model to represent attack scenarios [B. Schneier 1999]
  - **Root node**: main attack goal
  - **Refinement operators**:
    - AND - all children nodes to be done
    - OR - at least one children node to be done
    - SAND, K-of-N, etc.
- **Leaf nodes**: atomic attack steps

Example



[Mauw and Oostdijk 2005]

Attack trees

Theory
vs
Practical needs

Theory

- Formal underpinnings
  - **Semantics**: what is an attack tree, are 2 trees equivalent
  - **Extensions**: not only attack nodes, more refinement operators
  - **Quantitative analysis methods**: measuring attack scenarios

Attack tree process in practice

- **Design**: create a good tree
- **Interpretation**: read a tree
- **Use**: get value from a tree

Practice: Challenges

- **Design**: time-consuming, error-prone
- **Interpretation**: cognitive challenges, misconceptions
- **Use**: ROSI computation, missing data, justification to the customer

Tree design questions

- **NO PRECISE GUIDELINES**
  - how to structure the tree?
  - how to label nodes?
  - how to deal with repeating nodes?
  - what is the meaning of tree elements?

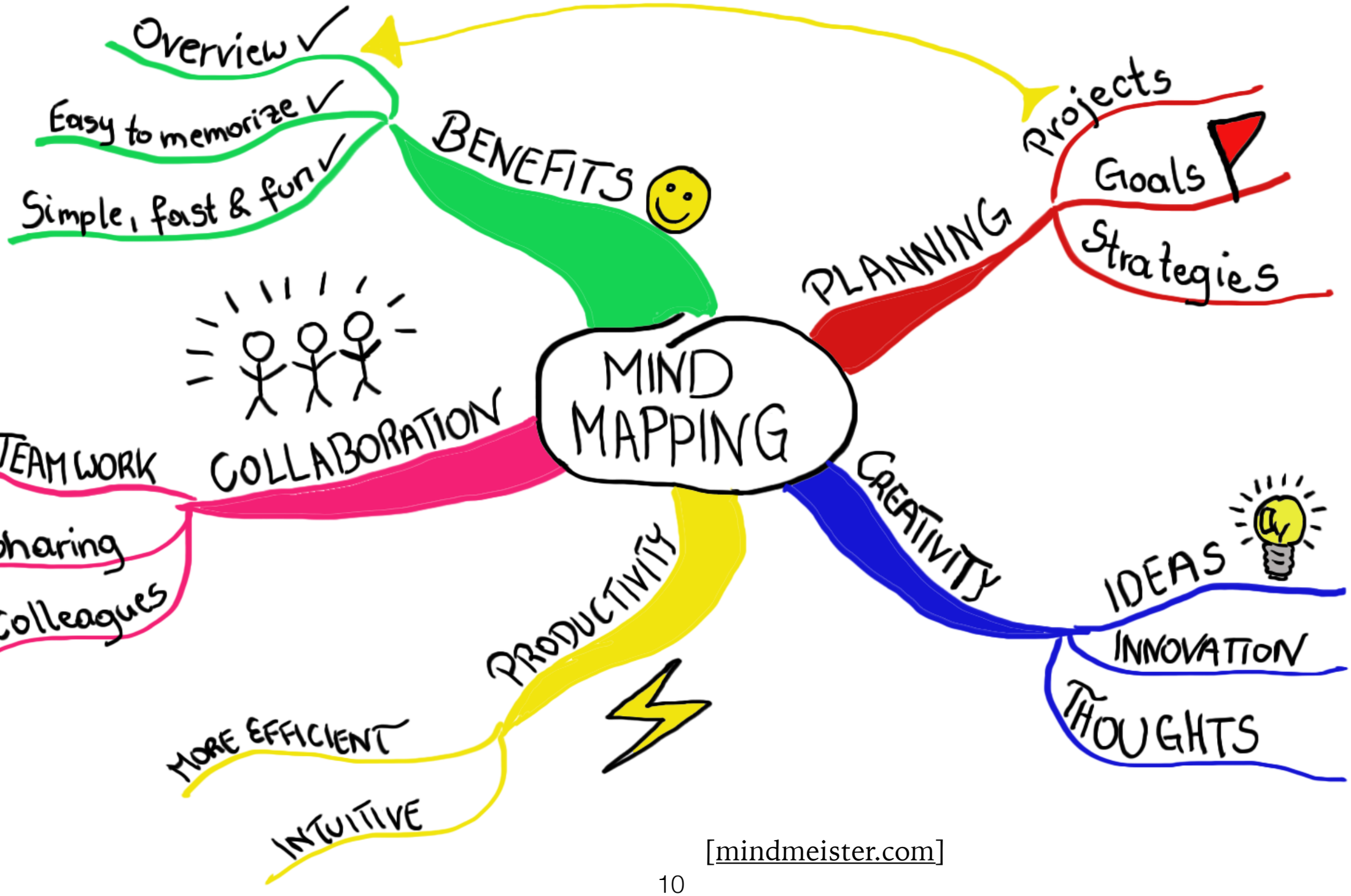
Attack tree value

- Facilitate brainstorming and communication across the board

“Attack tree is a mind map”

–Practitioner

Mind maps



[mindmeister.com]

More than a mind map

- Theory **boosts** practice
  - compute important attribute metrics and answer complex queries about attack scenarios
    - sensitivity analysis
  - reuse (sub-)trees

The attack tree formalism is not aligned with the practice

Steps in the right direction

- **Attack tree generation**: automatically generate a tree from a system model

- **Validation**: confirm that the tree is complete and sound wrt to the model; evaluate that the tree is correct with respect to the semantics, a threat catalogue, or data.

- **Visualisation**: show the tree in a comprehensible manner

- **Evaluation of the formalism:** investigate empirically whether attack trees facilitate threat modelling and how they do it

Theory vs Practice: what is an attack tree?

- Anything that complies with the definition is an attack tree
  - if a method generates something that complies with the definition, it is useful
  - even if this “tree” is huge and incomprehensible
- large, complete trees are good
  - allow to better express and analyse attacks

VS

- An attack tree is valuable for its refinement structure & as a communication means
  - higher-level nodes are more abstract attack elements than lower level ones
- a tree cannot be too big
  - difficult to comprehend and make decisions

Theory vs Practice: how to interpret a tree?

- Attack tree semantics are defined via combinations of leaf nodes

- **bottom-up** interpretation

VS

- Humans start with the top goal and refine it subsequently into lower level ones

- **top-down** reasoning

It’s now time to work on

- a more **rigorous methodology** for attack tree application in industry
  - find and eliminate the pitfalls
    - tree structure for comprehensibility; validation
- automated **generation approaches** that are more comprehensible and fit the industry process
  - refinement-aware, natural language-based, well-structured
- **empirical studies** of attack trees
  - a way to find many answers

Thank you!

olga.gadyatskaya@uni.lu