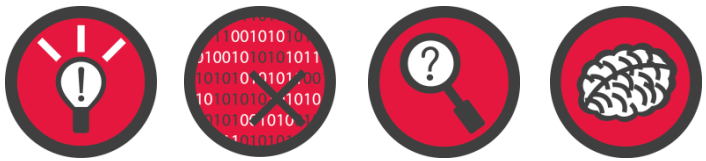


Fast and Optimal Countermeasure Selection for Attack Defence Trees

18.10.2016

RISK16 workshop

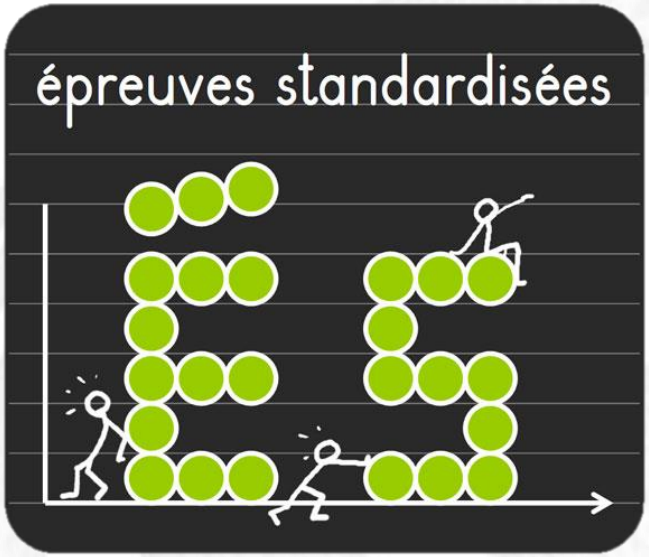
Steve Muller
Carlo Harpes
Cédric Muller

itrust consulting s.à r.l.
55, rue Gabriel Lippmann
L-6947 Niederanven

Tel: +352 26 176 212
Fax: +352 26 710 978
Web: www.itrust.lu

Fast & Optimal Countermeasure Selection

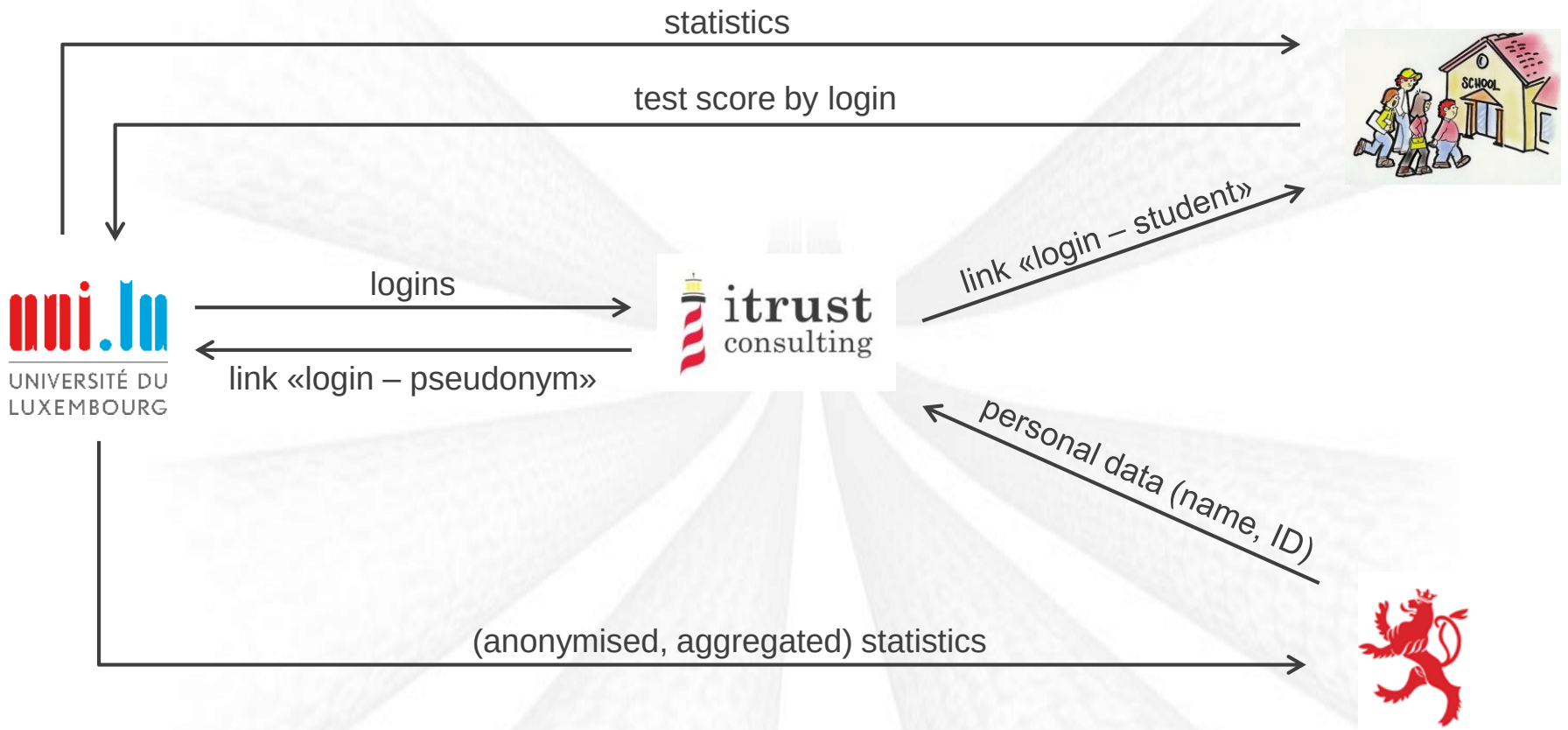
Risk context: ÉpStan



Monitor the **quality** of the **educational system** of secondary school

Fast & Optimal Countermeasure Selection

Risk context: ÉpStan



pseudonym

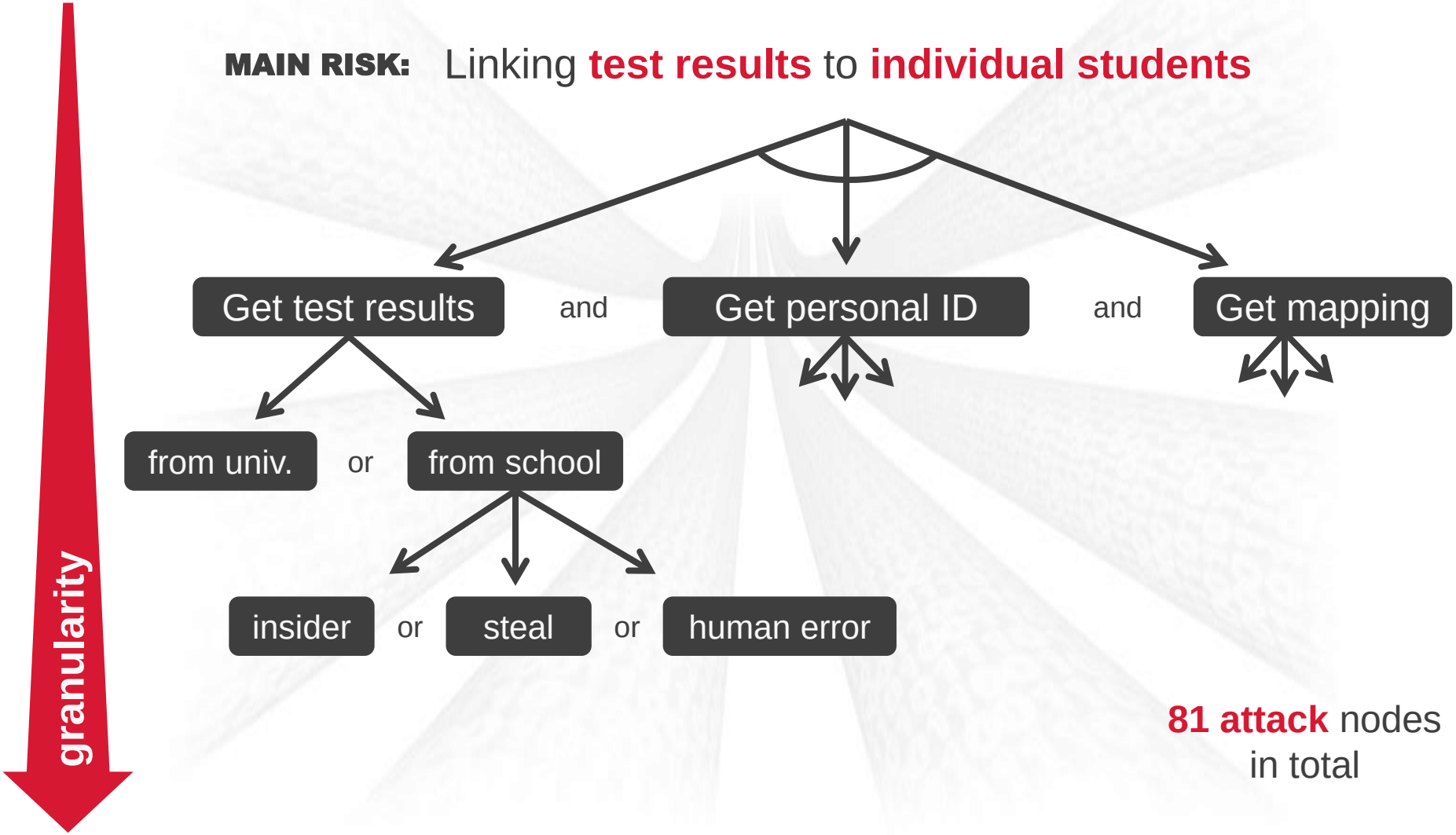
personal data

results

results

Fast & Optimal Countermeasure Selection

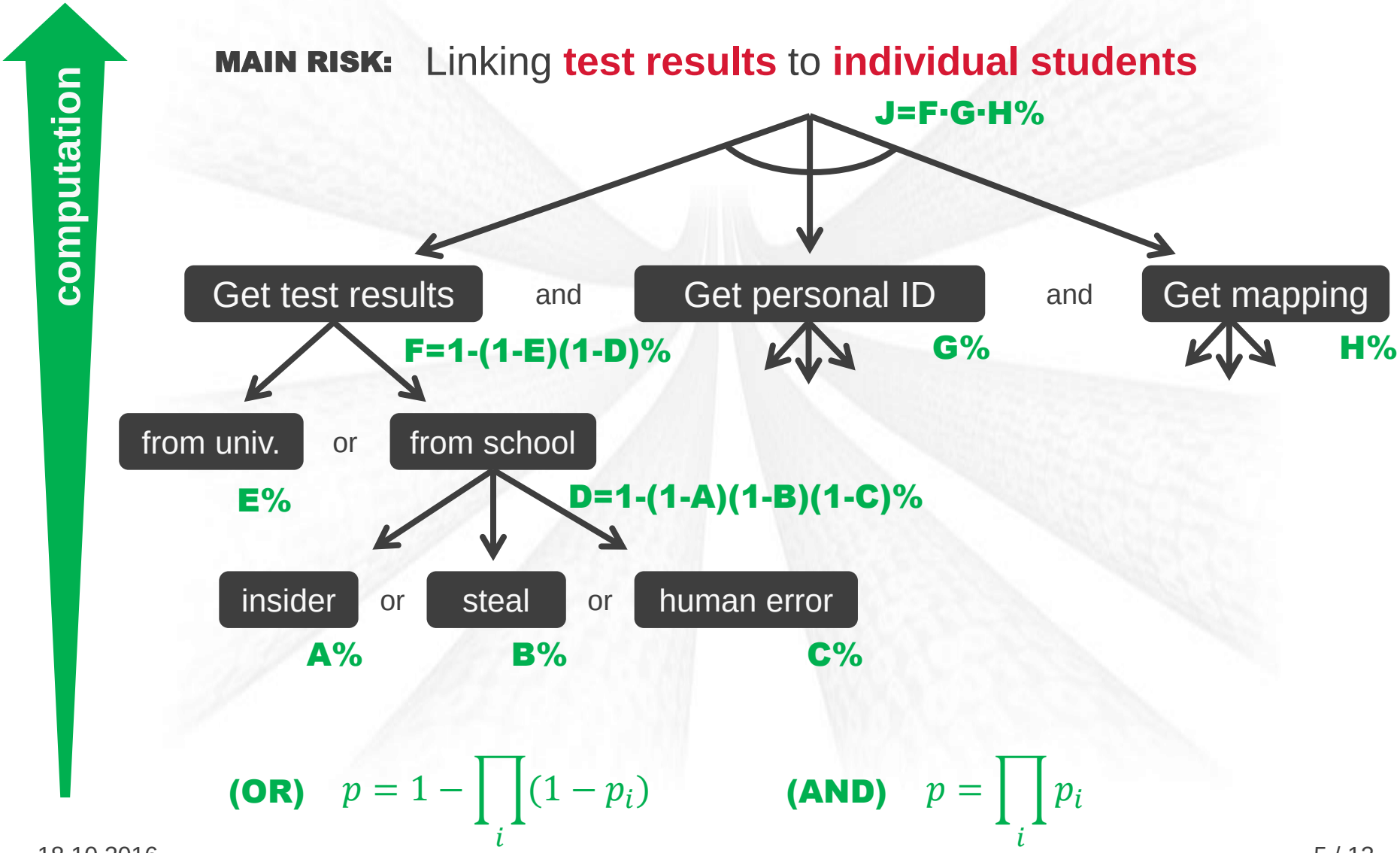
Attack Tree



81 attack nodes in total

Fast & Optimal Countermeasure Selection

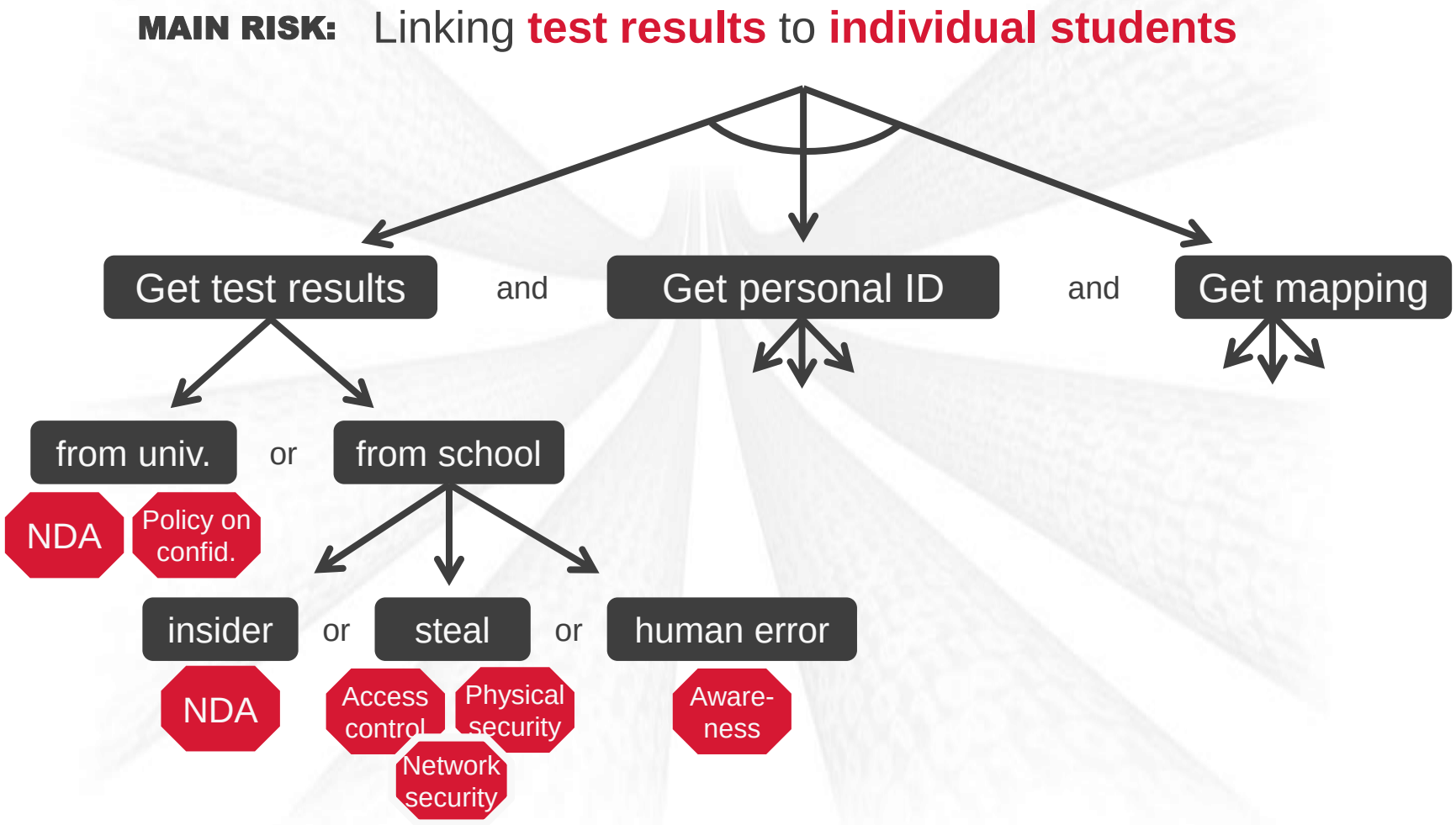
Attack Tree



(OR) $p = 1 - \prod_i (1 - p_i)$ **(AND)** $p = \prod_i p_i$

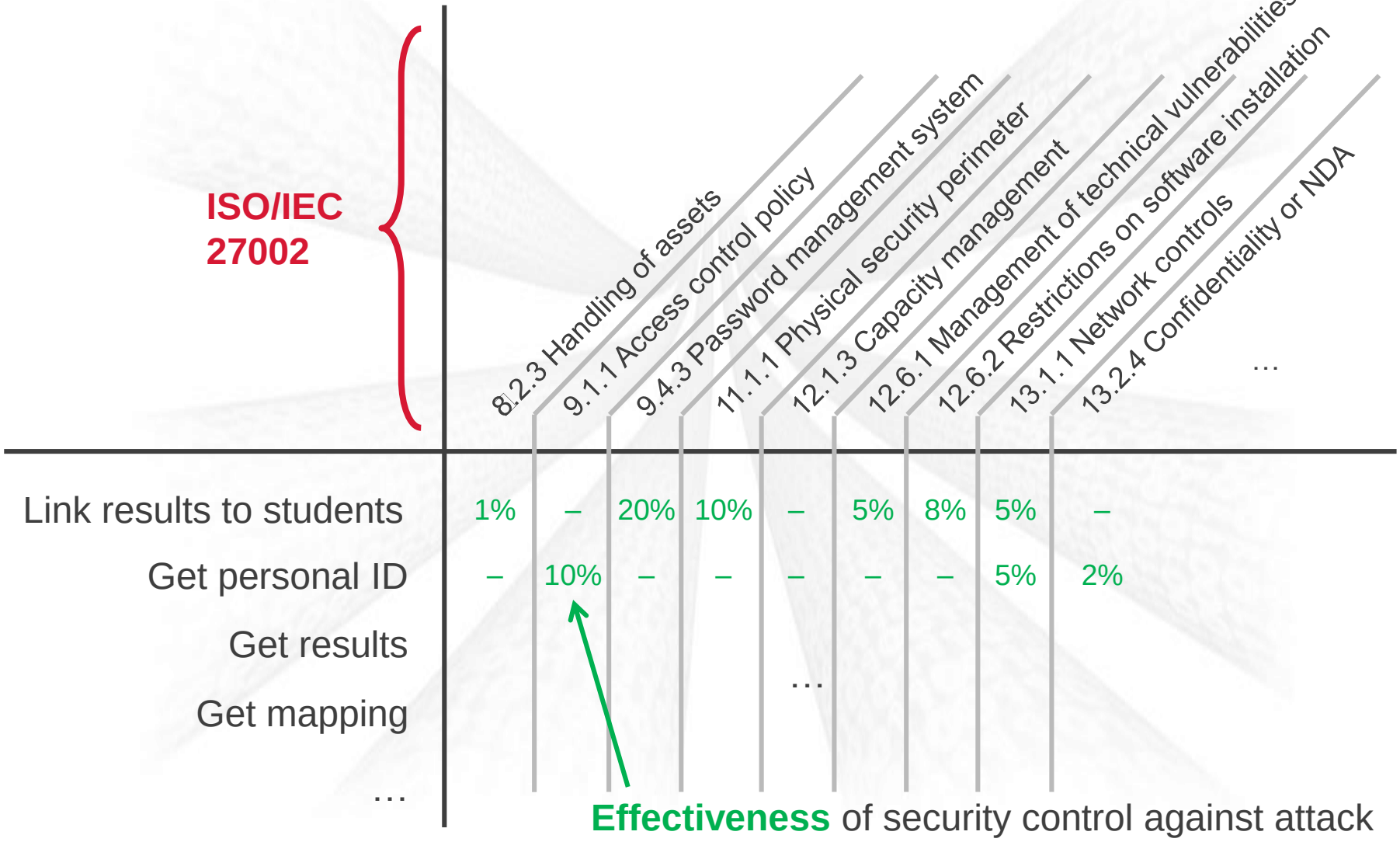
Fast & Optimal Countermeasure Selection

Attack *Defence* Tree



Fast & Optimal Countermeasure Selection

Defences



Fast & Optimal Countermeasure Selection

Optimal countermeasure selection

	add defence	remove defence
RISK **Probability** [*link test results*] × **Impact** [*link test results*]	↓	↑
COST **Sum of costs** *of implemented defences*	↑	↓

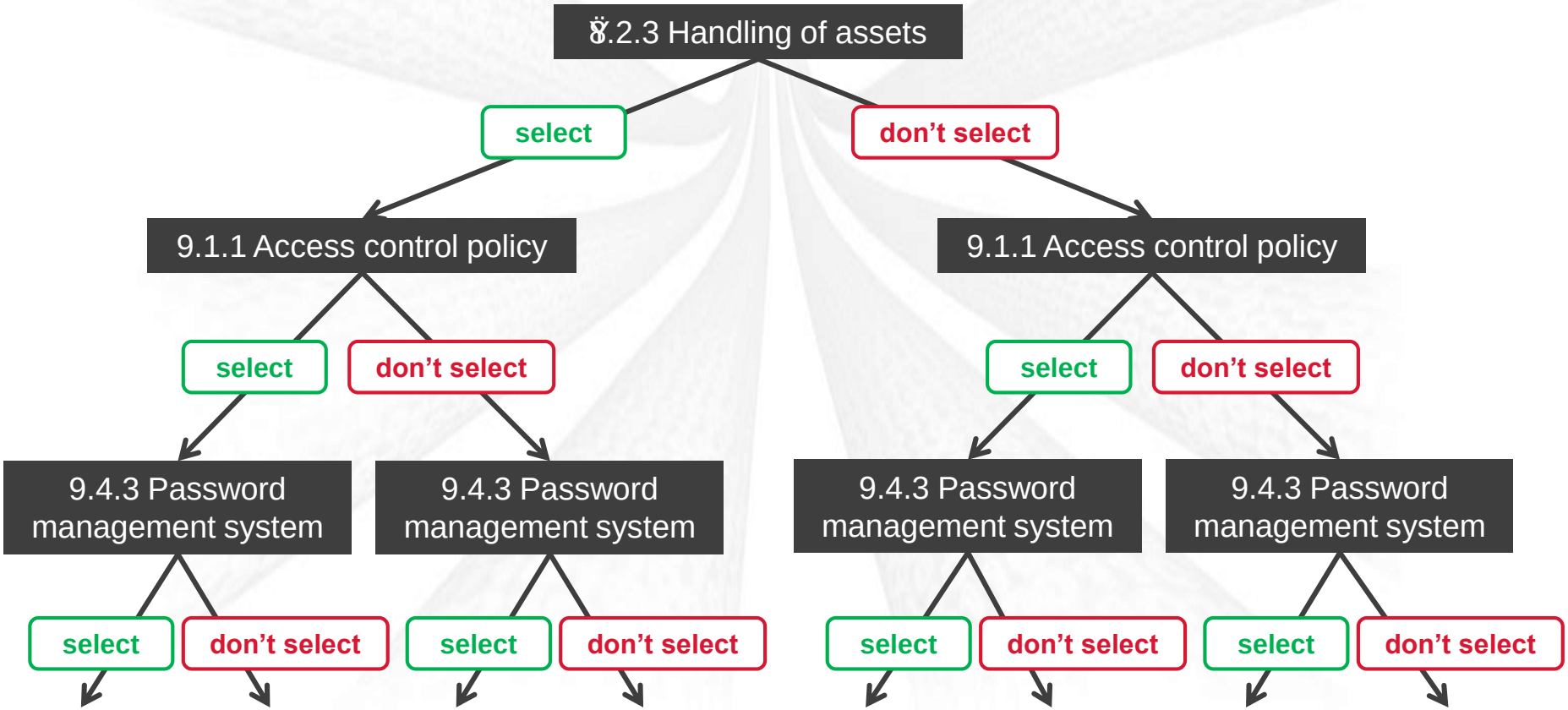
OPTIMISATION PROBLEM

Which countermeasures **reduce risk** best at the **lowest cost**?

Fast & Optimal Countermeasure Selection

Naïve algorithm

Brute-force: Try out all combinations of selecting counter-measures



Fast & Optimal Countermeasure Selection

Naïve algorithm

itrust consulting

Problem: Needs 2^n iterations for n counter-measures

$3{,}32 \cdot 10^{35}$ iterations for **118** counter-measures

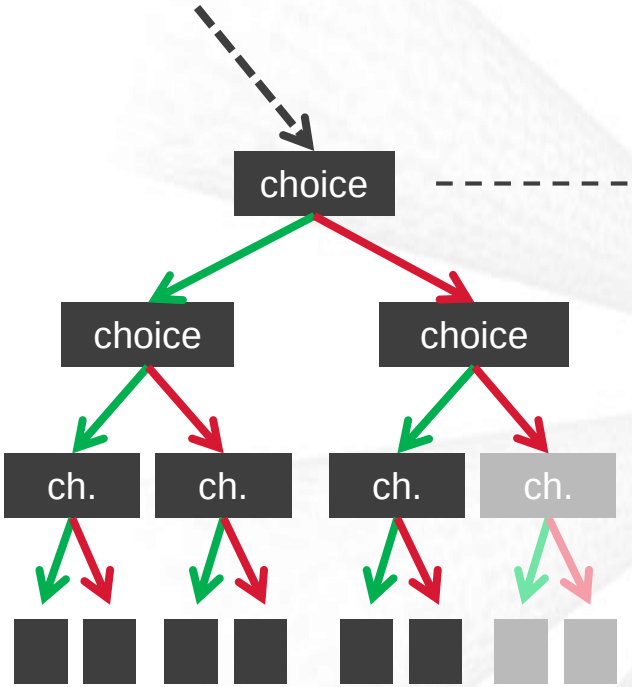
(unfeasible to compute)

$1{,}10 \cdot 10^{12}$ iterations for **40** counter-measures

(**13 days** with 1 iteration per millisecond)

Fast & Optimal Countermeasure Selection

Improved algorithm



Subsequent choices will:

- Increase number of defences
- **Reduce risk**

Once a defence becomes unprofitable, it will remain unprofitable.

→ **Can skip all further combinations**

Fast & Optimal Countermeasure Selection

Improved algorithm: Performance

	random attack-defence tree	ÉpStan use-case
Naïve brute-force	—	54,2 seconds
Brute-force with data structure	$4 \cdot 10^{15}$ years	0,92 seconds
Branch and bound	**15 minutes**	**0,36 seconds**
	(81 attacks, 90 defences, 7290 effectiveness values)	(81 attacks, 16 defences, 58 effectiveness values)

Fast & Optimal Countermeasure Selection

Thank you.

This work was supported by the European Commission's Seventh Framework Programme (FP7/2007-2013) under grant agreement number 318003 (TREsPASS).

This work was supported by

Fonds National de la Recherche Luxembourg

(project reference 10239425)