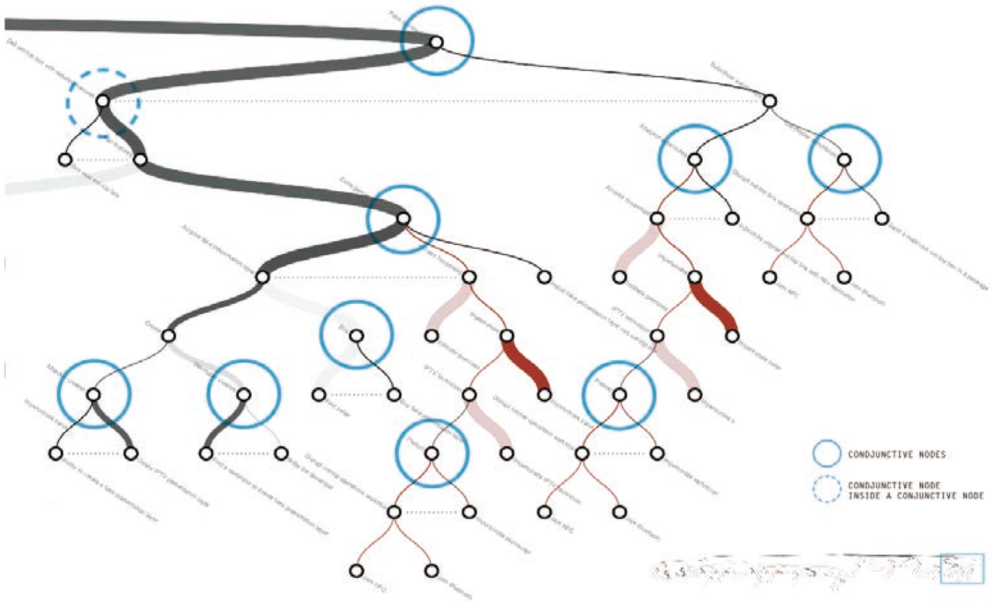
Model-based Risk Management for Socio-Technical Systems – Report on the TRE$_S$PASS Project

predict
prioritise
prevent

TRESPASS



SEVENTH FRAMEWORK PROGRAMME

Dieter Gollmann
Hamburg University of Technology

European Commission

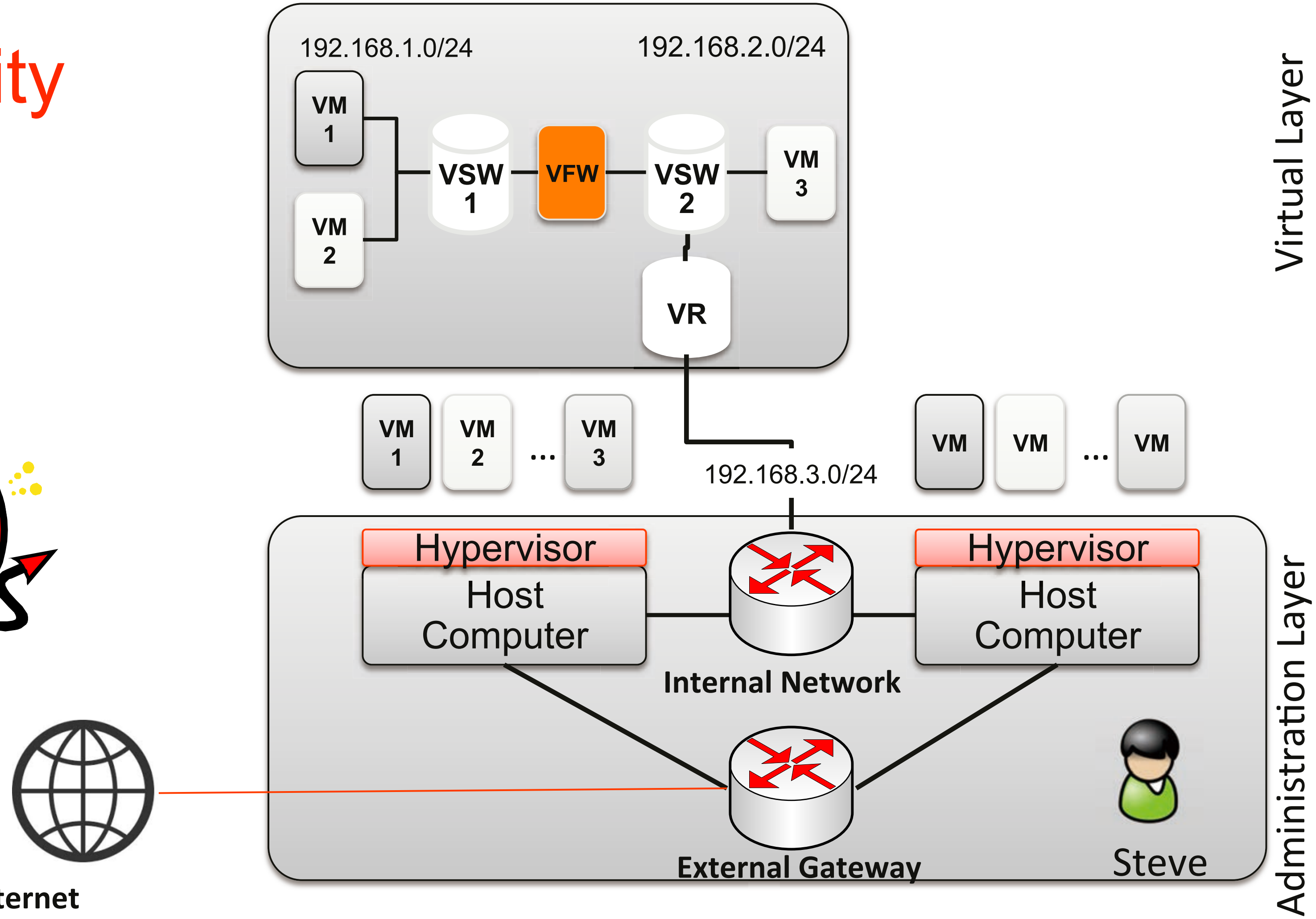
About the speaker

- PhD on a topic in cryptography, 1984
- Research on cryptographic algorithms & protocols, foundations of computer security, risk analysis
  - Container transport, German e-health card, now TRE$_S$PASS
- Course director, MSc in Information Security, Royal Holloway, University of London, 1992 – 1997
- Microsoft Research Cambridge, 1998 – 2003
- Chair for Security in Distributed Applications, Hamburg University of Technology, since 2003
- Now JSPS Invitational Fellowship at Kyushu University

Agenda

- My views on the intrinsic challenges in risk management
- Report on the way these challenges are addressed in the EU research project “Security is a people problem”
  - Be they part of the problem, be they part of the solution, people should be part of the model
- Acknowledgement: talk uses slides from project partners
- Talk gives my view, not necessarily the project’s view

From
IT security



Towards socio-technical systems

skills

goals

resources

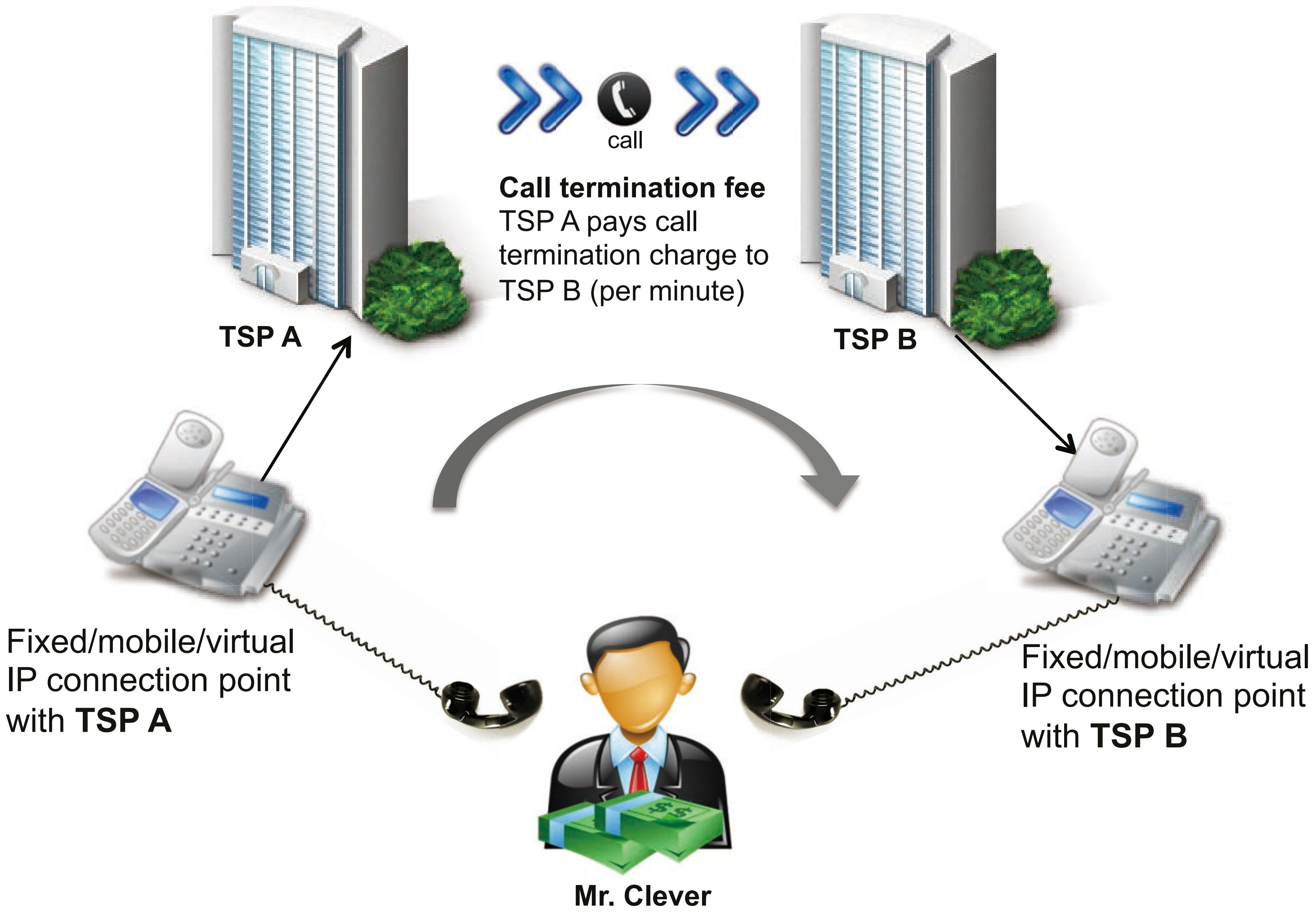
TRE$_S$PASS project 2012-2016

- EU FP 7 Integrated Project, funding ≈ € 10,000,000
- Seventeen partners, large companies, SMEs, academia
- Expertise ranges from visualization to model checking to criminology

TRE$_S$PASS use cases

- Use cases to guide the project
- Obtained from industry partners and industry contacts
- For validating methods and tools developed
- To pose new research questions

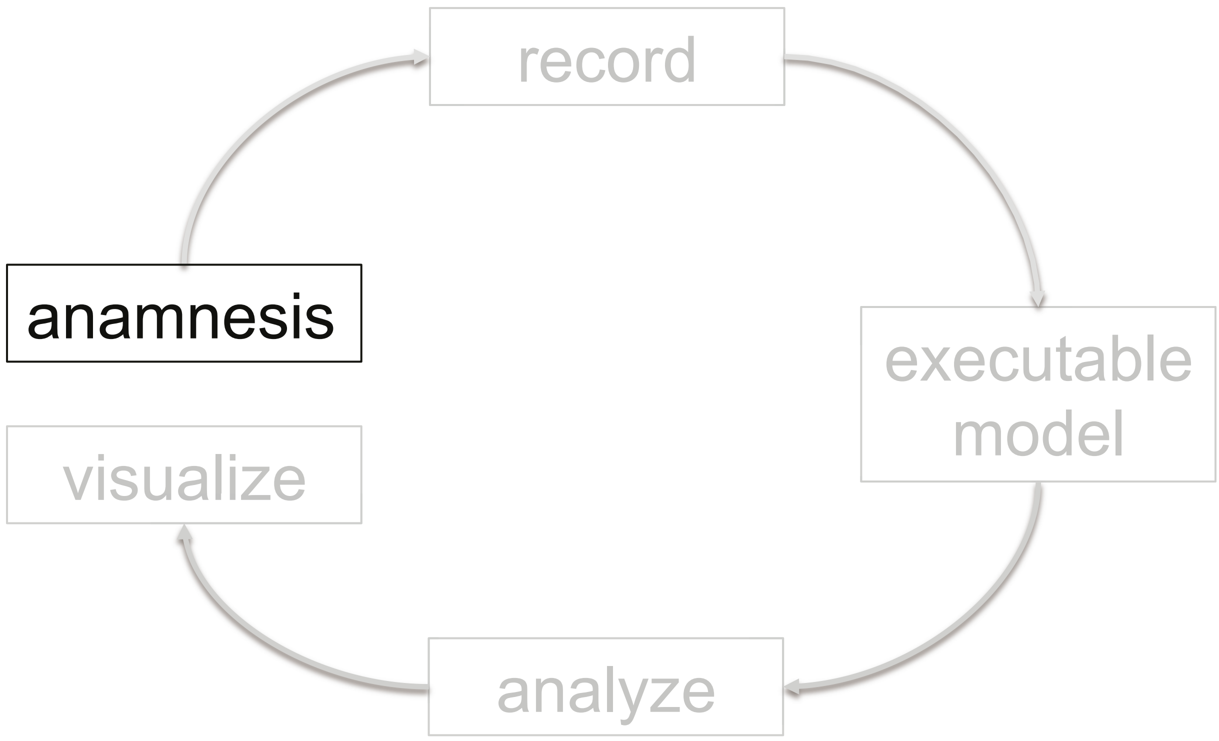
Parasitic business models
(tariff misuse of call termination)



Model-based risk management

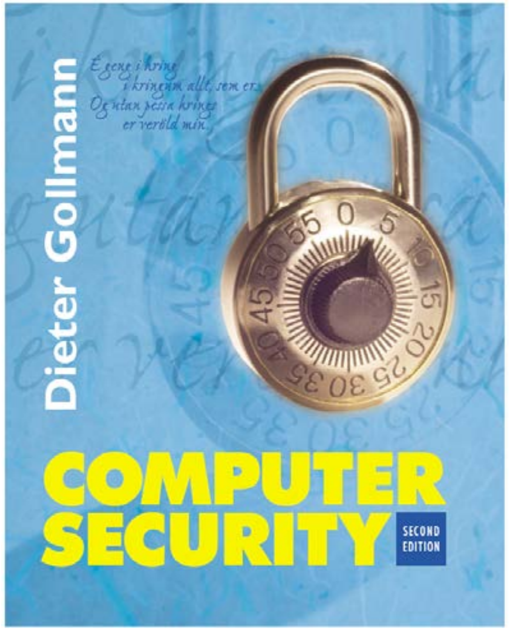
- Capture requirements – anamnesis
- Model system / organization, requirements, attacker
- Construct executable models
- Evaluate, analyze, communicate (visualize)
- Decide

Capture requirements



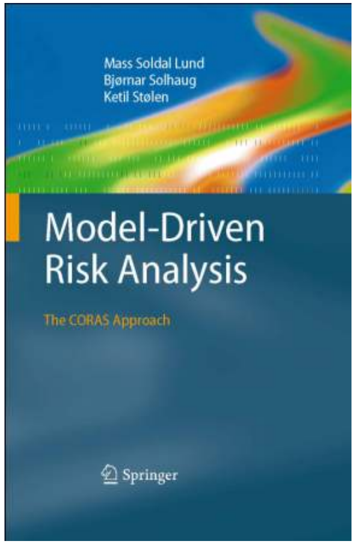
Fundamental dilemma of computer security

- **Security unaware** users have specific security requirements but usually no security expertise
- Risk management is communication
- How to get this communication started?



Facilitating communication

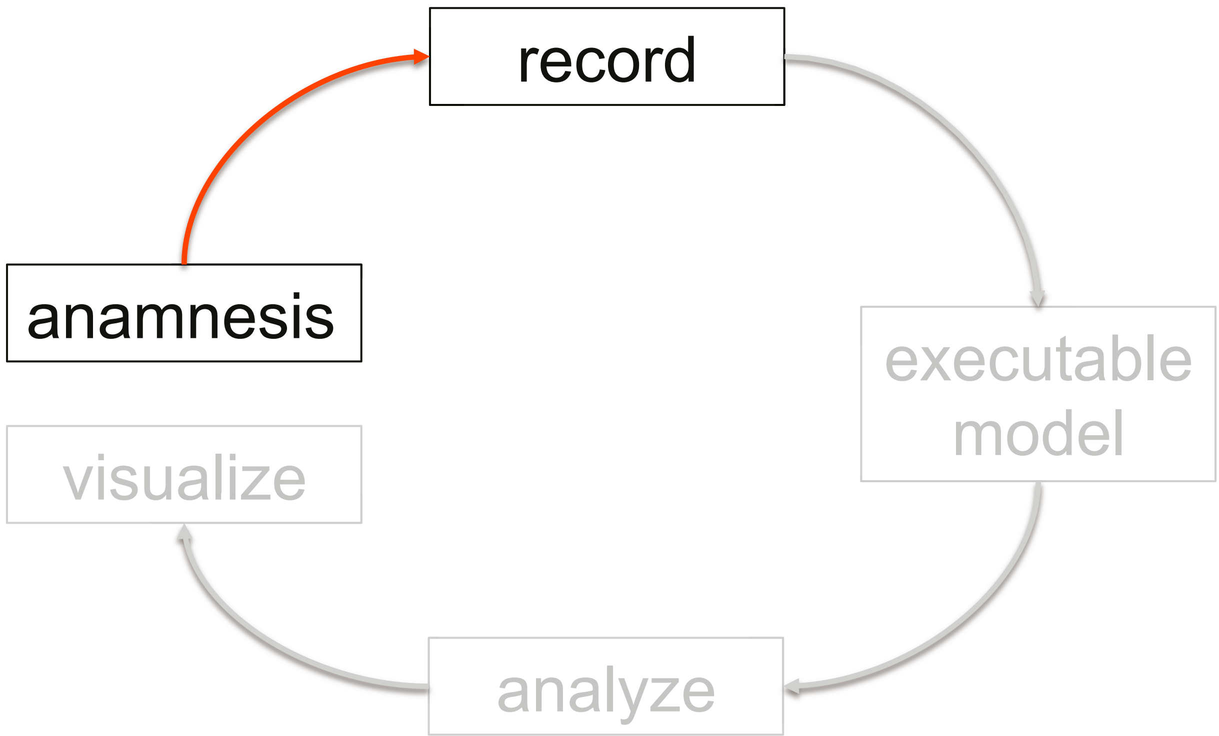
- CORAS: earlier EU project on model-based risk analysis
  - Stage 1: staff describes organization to security experts
  - Stage 2: security experts describe organization to its staff



- TRE$_S$PASS
  - Explores use of Lego building blocks in brainstorming sessions

http://heim.ifi.uio.no/~ketils/coras/index.htm

Model organization



Fundamental challenge in model-based risk analysis

- **Capturing and aligning two intrinsically different views of a system, the operator’s view and the attacker’s view**

- Operator’s view framed by intended use of the system
  - Includes features relevant for describing operation of the system
  - May include defenses against anticipated types of attacks
- Attacker’s view
  - Can be approached in two ways

Attacker's view – 1

- Extend operator's view: attack points and attack patterns
  - Alignment of the two views is comparatively easy
  - View on attacks may be blinkered by too much familiarity with intended use of the system ("Betriebsblindheit")
  - May miss attacks exploiting features outside of the system model
- Artful attackers explore gaps between operator's model and actual system to find levers for an attack
  - If it is provably secure, it probably isn't [Lars R. Knudsen]
  - Models are abstractions; gaps MUST exist

Attacker’s view – 2

- Create attacker’s view independently of operator’s view
- Some information about the system must be available
- Attacks identified at this stage may turn out to be infeasible because of specific features of the system under analysis that had not been considered
  - “But this attack is not possible because …”
  - System model needs to be refined
- Aligning the two views tends to be more challenging

TRE$_S$PASS system model
(operator's view)

- Represented as a directed graph
- Nodes can be
  - Locations, in physical space (e.g. rooms) or in cyberspace (e.g. network nodes, virtual machines)
  - Actors, e.g. people and processes; these nodes can move
  - Assets, can be attached to locations or actors, can be annotated with metrics
- Edges define various physical and logical connections
- Description language with formal semantics

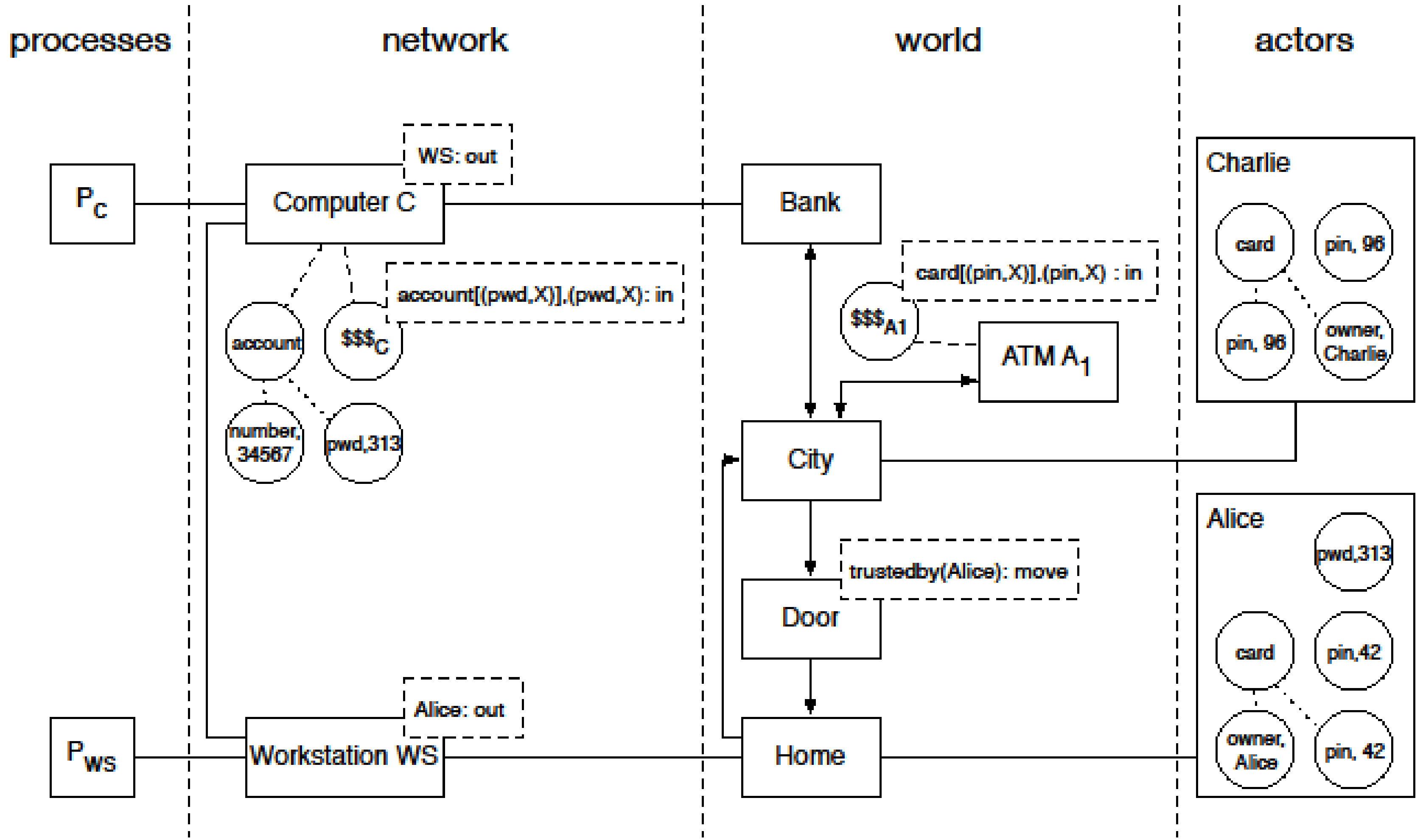
TRE$_S$PASS system model – quantities

- For actions, time to perform action, risk of detection when performing it, and cost of performing it
- For actors, likelihood of a social engineering attack to be successful and risk appetite of actor
- For locations, risk of detection at this location (for example due to surveillance cameras)

TRE$_S$PASS system model
– behavior and policies

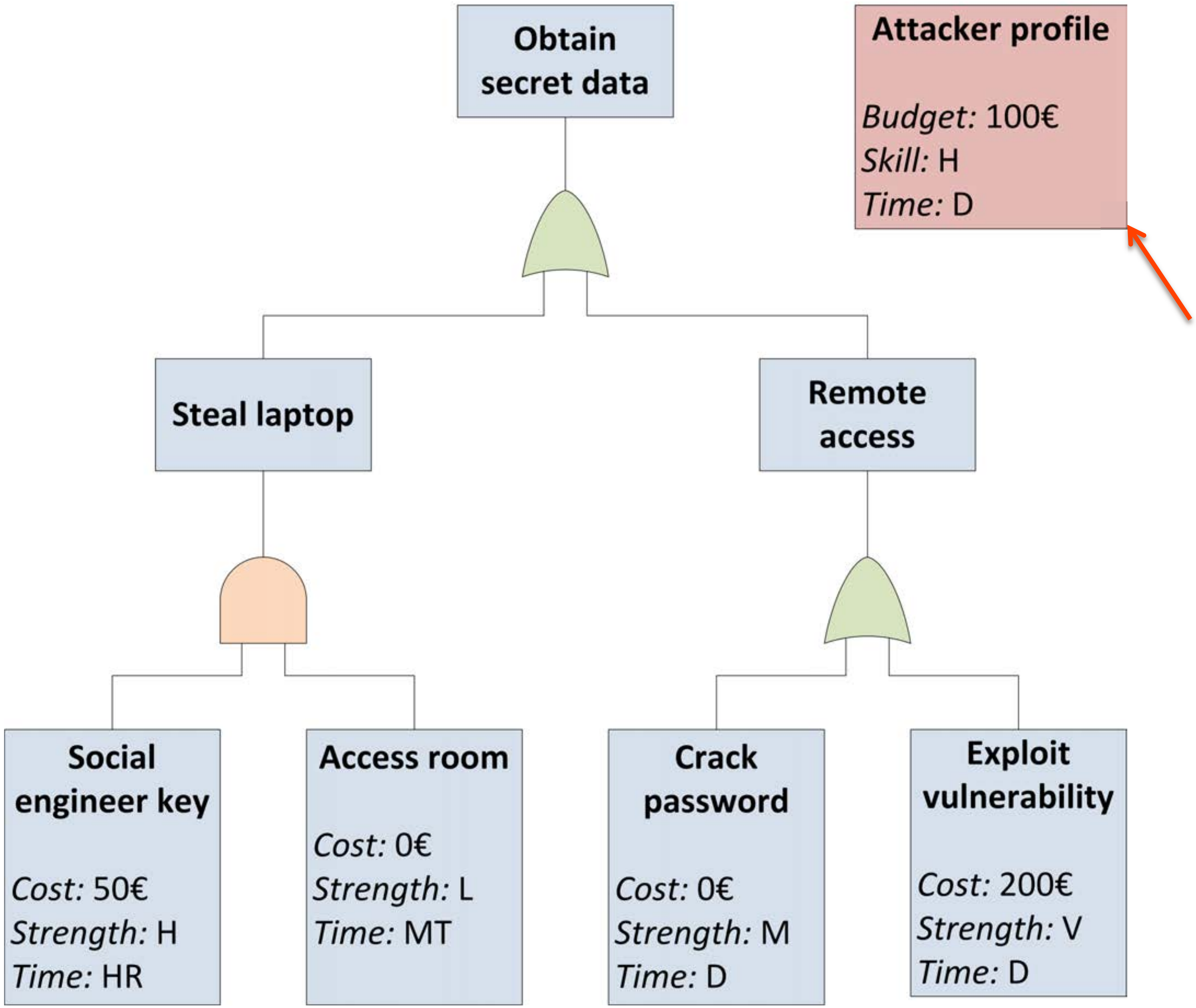
- Domains limit where processes can move
  - Human actors restricted to room nodes, computer processes restricted to network nodes
- Possible to define the behavior of actors
- Policies, both access control policies and security goals
  - “To access the account, a PIN is required”
  - “This data item must remain confidential”
- Attacks treated as policy violations

TRE$_S$PASS system model – example

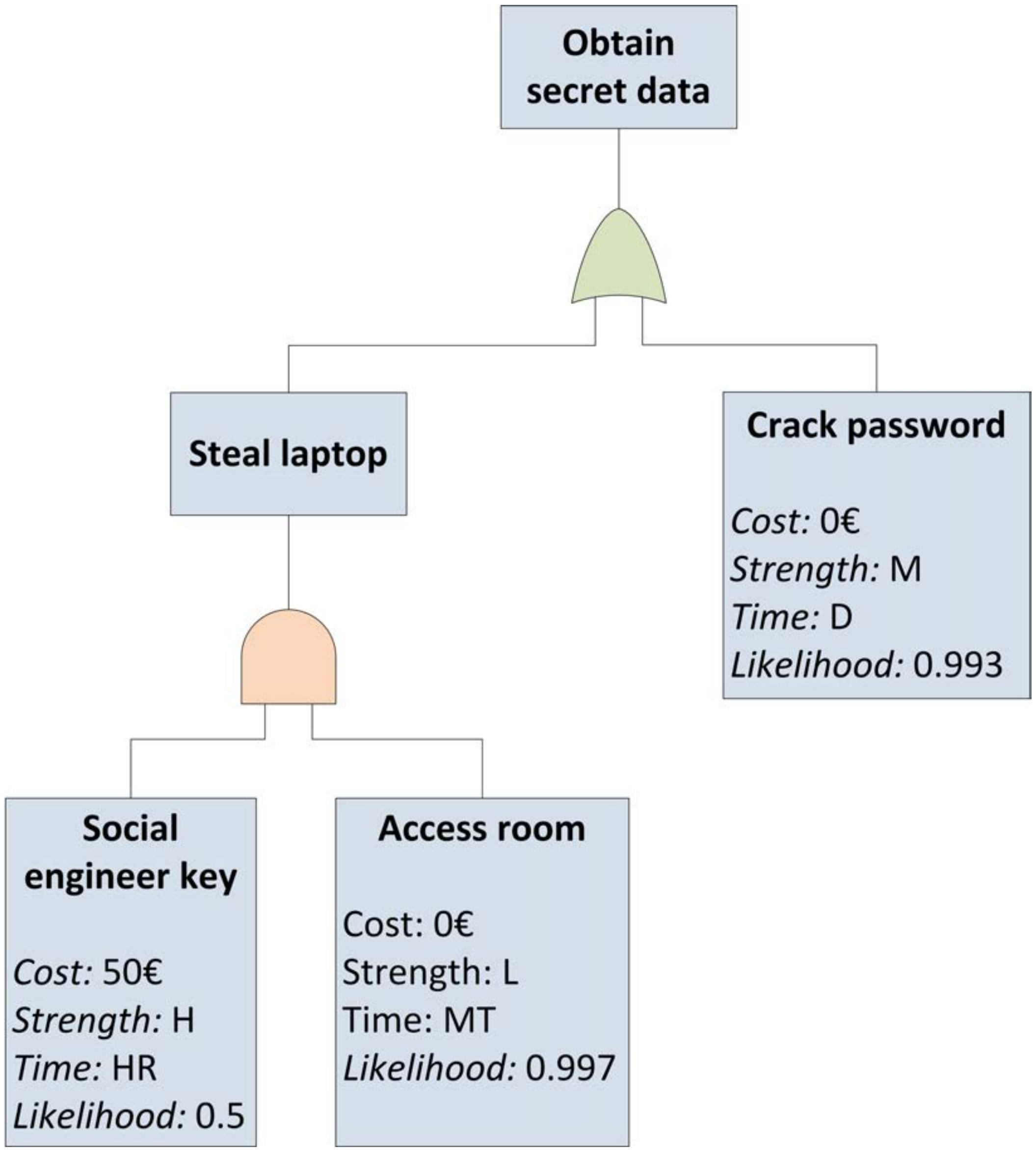


Attacker's view

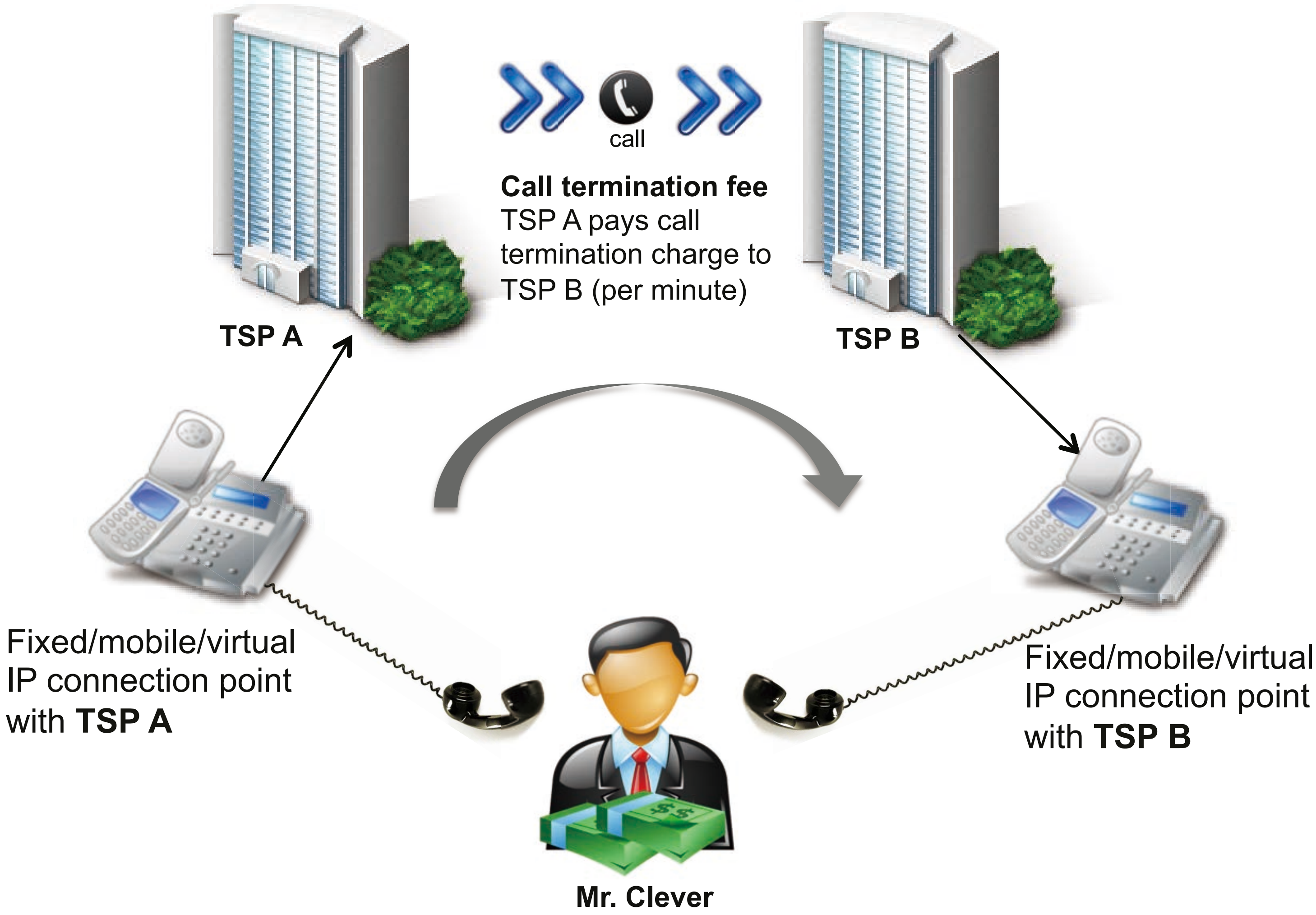
- Attack trees for structuring brainstorming about attacks
- Attack tress augmented with
  - Attributes: likelihood, cost, time, skill level, …
  - Defense nodes (attack-defense trees, also work in TRE$_S$PASS)
- Tool support (also work in TRE$_S$PASS, ADTree tool)
- E.g. pruning of trees with respect to attacker profiles



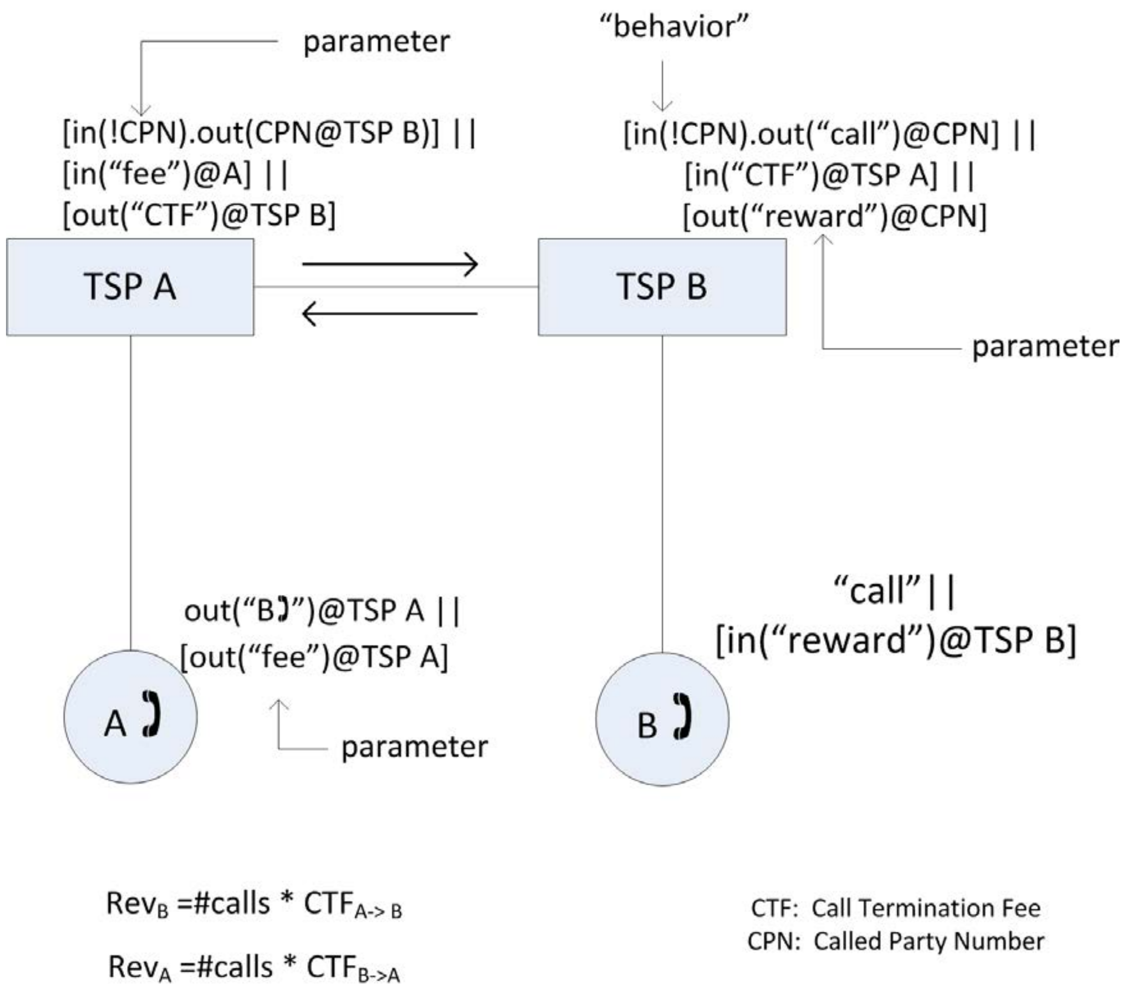
Obtain secret data
Attacker profile
Budget: 100€
Skill: H
Time: D
Steal laptop
Remote access
Social engineer key
Cost: 50€
Strength: H
Time: HR
Access room
Cost: 0€
Strength: L
Time: MT
Crack password
Cost: 0€
Strength: M
Time: D
Exploit vulnerability
Cost: 200€
Strength: V
Time: D


Obtain secret data
Steal laptop
Crack password
Cost: 0€
Strength: M
Time: D
Likelihood: 0.993
Social engineer key
Cost: 50€
Strength: H
Time: HR
Likelihood: 0.5
Access room
Cost: 0€
Strength: L
Time: MT
Likelihood: 0.997

Parasitic business models
(tariff misuse of call termination)



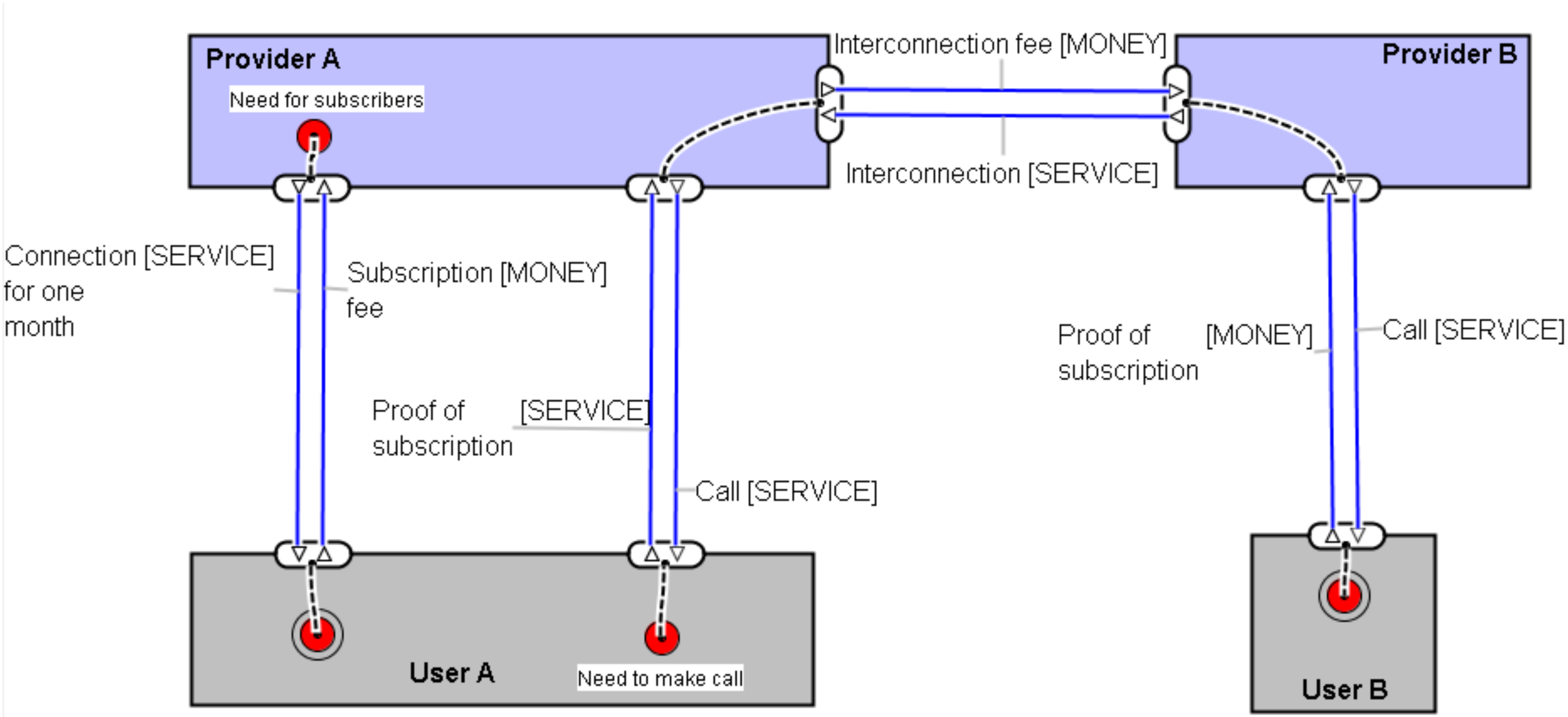
TRE$_s$PASS model



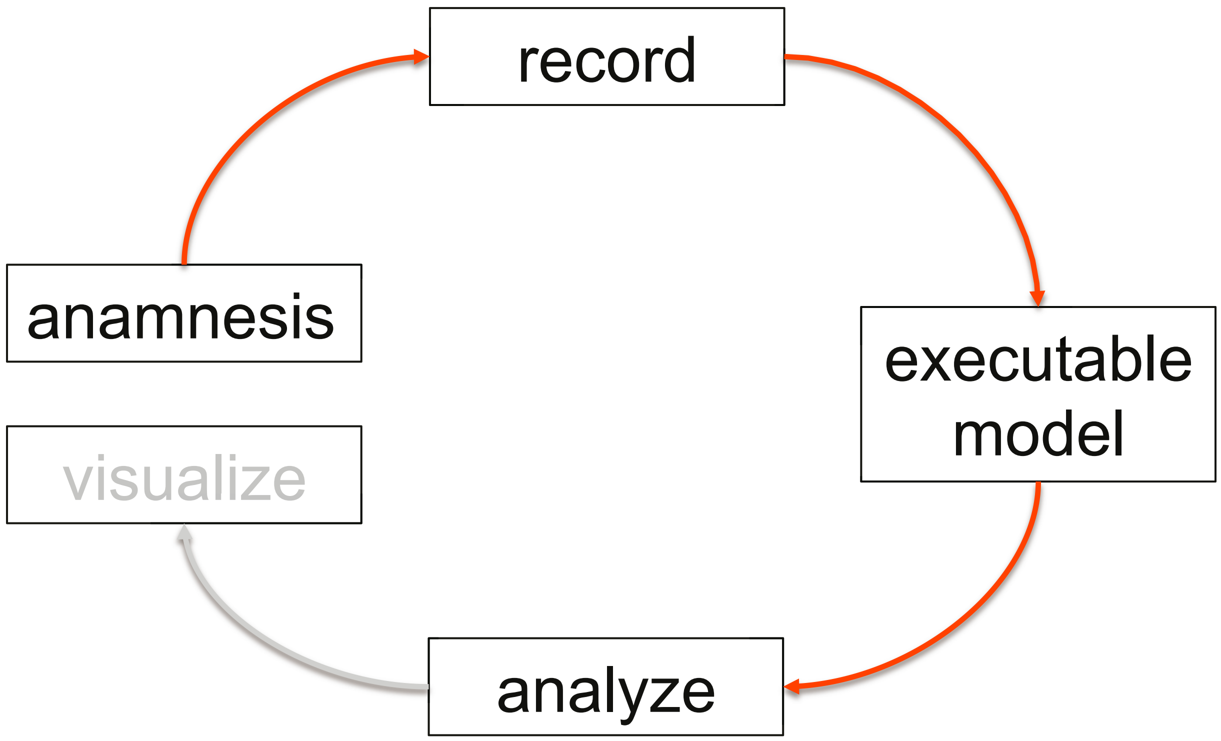
Actions	Description
in	Waiting for incoming action
out	Outgoing action to other actors

Operators	Description
!	Waiting for an input
dot(.)	Sequential actions
||	Executing actions in parallel
@	"from" where the action is performed

Value modelling using e3fraud



Analysis



Fundamental challenges in analysis and evaluation

- How to deal with uncertainty?
- How to deal with complexity?
- How to deal with dependencies?
- How to achieve completeness?

Uncertainty

- How to model uncertainty?
  - Subjective probabilities (Bayesian approach)?
  - Frequencies (frequentist approach)?
  - Other mathematical frameworks, fuzzy theory, etc.?
- Do we have the data and do probabilities work at all?
  - Expectations that mandatory reporting will improve the situation
  - Current disillusion in the UK about data-driven approach
  - "We had lots of data on the financial markets but did not foresee the crisis of 2008 …"
  - "In security the past is a poor indicator of the future!"

Complexity

- Divide-and-conquer is a powerful strategy
  - E.g., attack trees break down a high-level goal into basic actions
  - Easier to assign metrics to basic actions than to high level goals
- How to return from divide-and-conquer?
  - Methods for combining metrics for subsystems to achieve compositionality
- How to deal with dependencies?

Completeness

- How to avoid missing out on attacks?
- Brainstorming is a creative but informal process, may miss attacks that are obvious in hindsight
- TRE$_S$PASS explores the use of model checking for systematic attack discovery

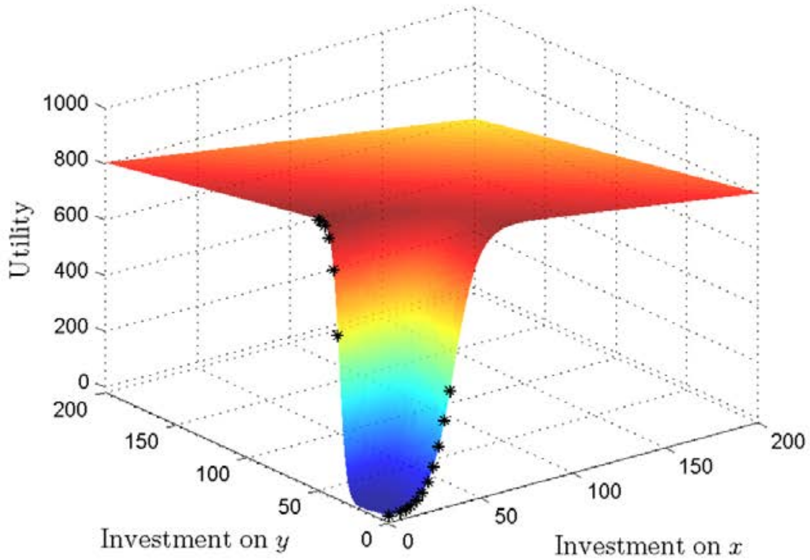
TRE$_S$PASS analysis methodology

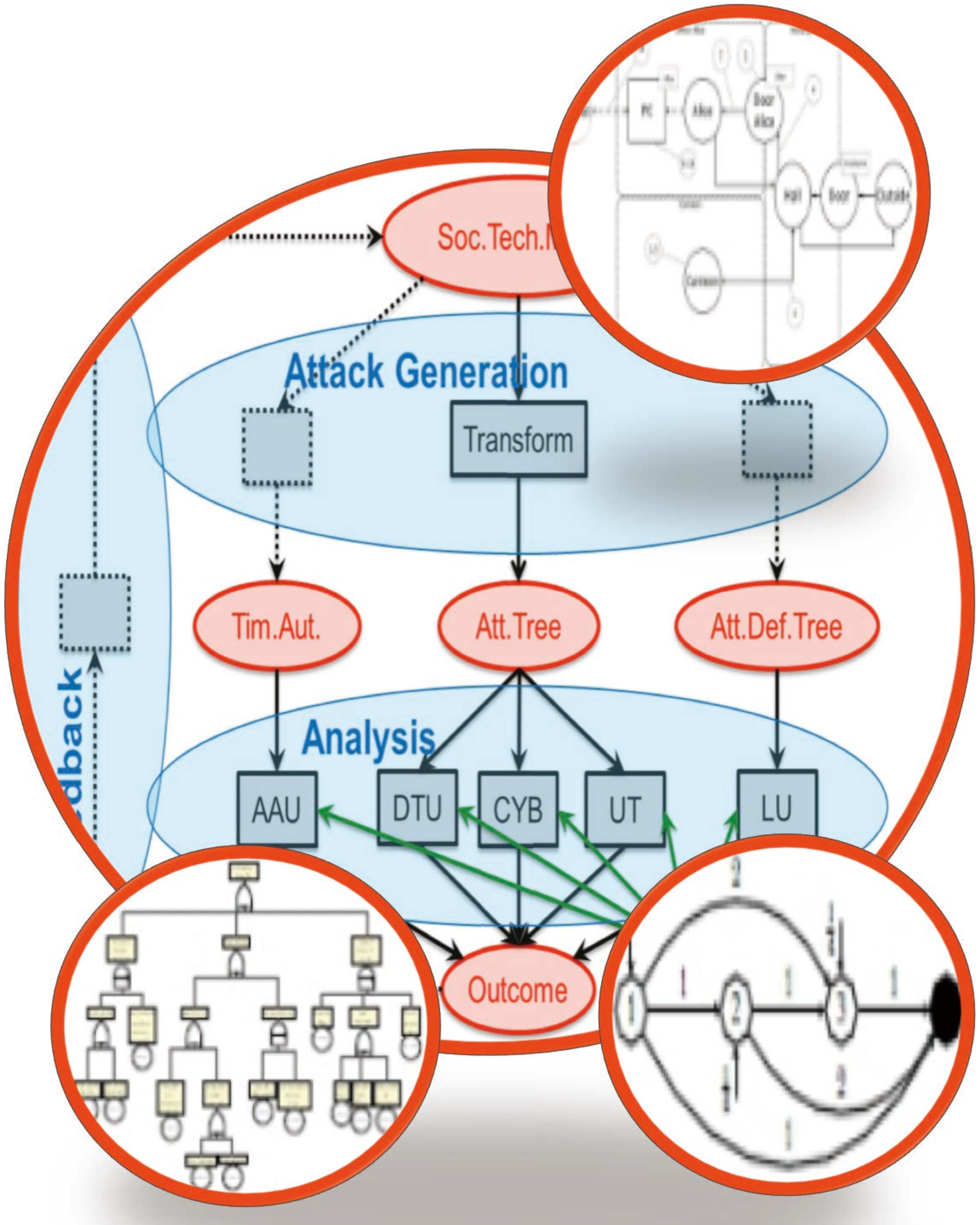
- Start from an attack tree
- Convert attack tree into an executable stochastic model
  - Interactive Markov chains
  - Markov automata (choice + time-dependent success probability)
  - Priced (weighted) timed automata (basis for model checking)
- Check for security properties in the executable model
  - Ideally, cover all possible executions of the system

TRE$_S$PASS analysis methods (sample)

- Computational analysis methods for attack trees
  - Extended to attack-defence trees
  - Pareto-optimal solutions considering multiple attributes
- Statistical model checking of timed automata
  - Derive results from several simulations of the system
  - Scales better than normal model checking
  - Deals with uncertainties in input values
- Model checking for policy violations
  - Delivers attack traces if a violation is found
  - Deals with completeness

Analyse


1000
800
600
400
200
0
Utility
200
150
100
50
0
Investment on y
0
50
100
150
200
Investment on x


Soc.Tech.
Attack Generation
Transform
Tim.Aut.
Att.Tree
Att.Def.Tree
Analysis
AAU
DTU
CYB
UT
LU
Outcome
dback

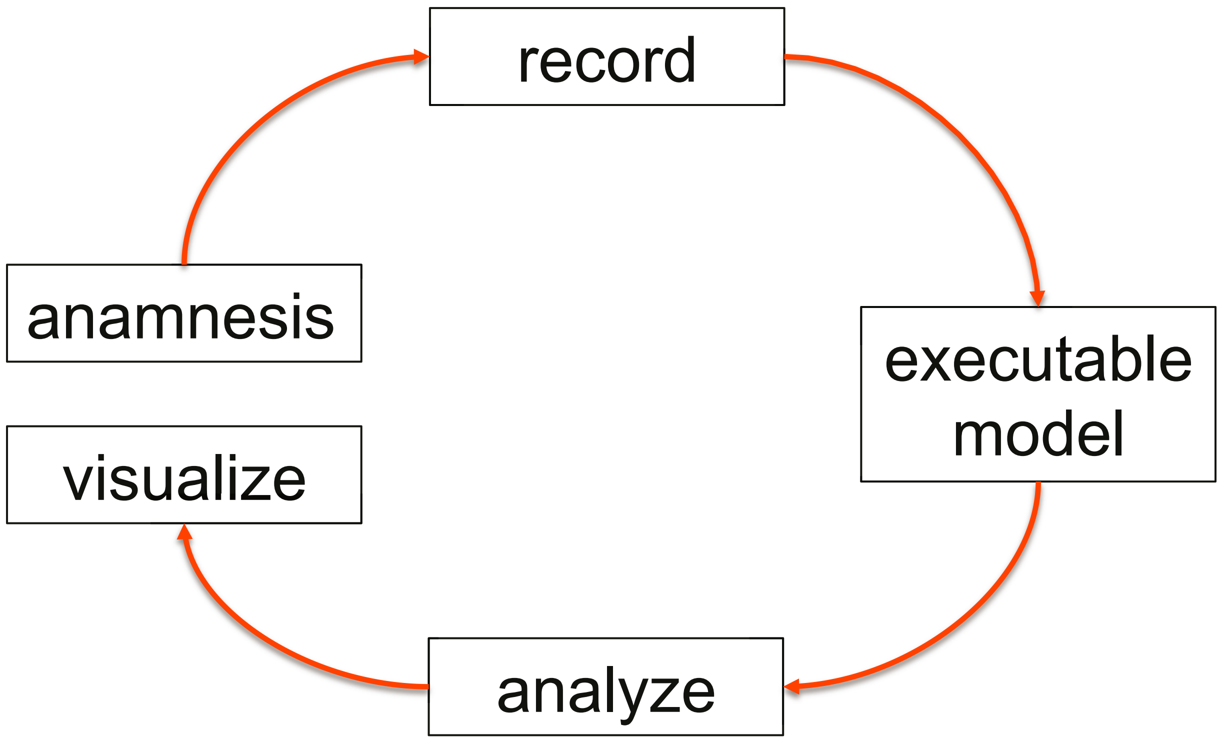
Understanding human actors

- Experiments on stealing laptops (in the past) and door keys (within TRE$_S$PASS) at Twente University
- Prevention campaign in key experiment significantly reduced vulnerability of people in an office environment
- Key-fob reduced cases of handing over a key to an attacker from 62.5% to 37%

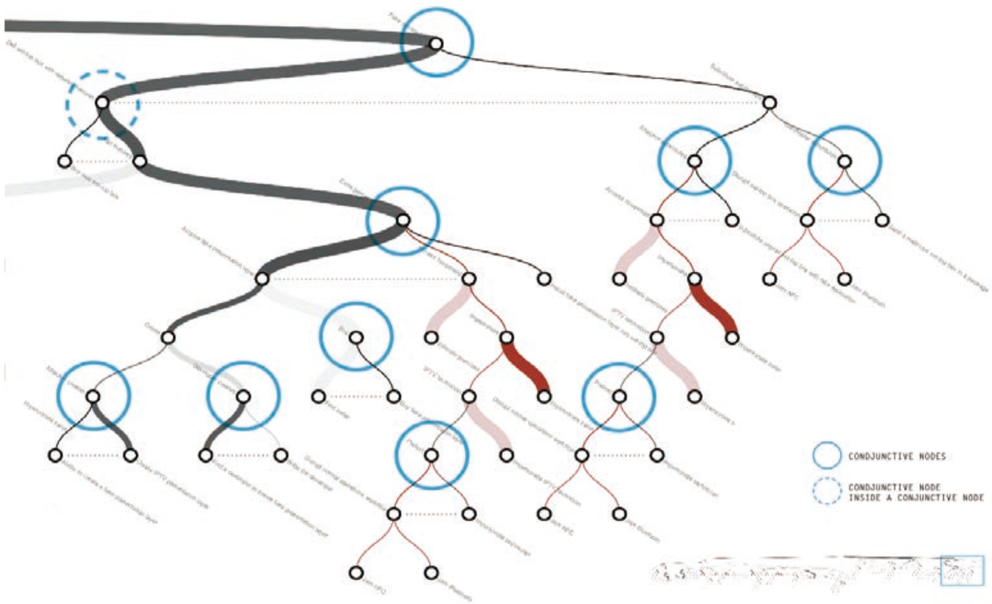
Cues and warnings experiment

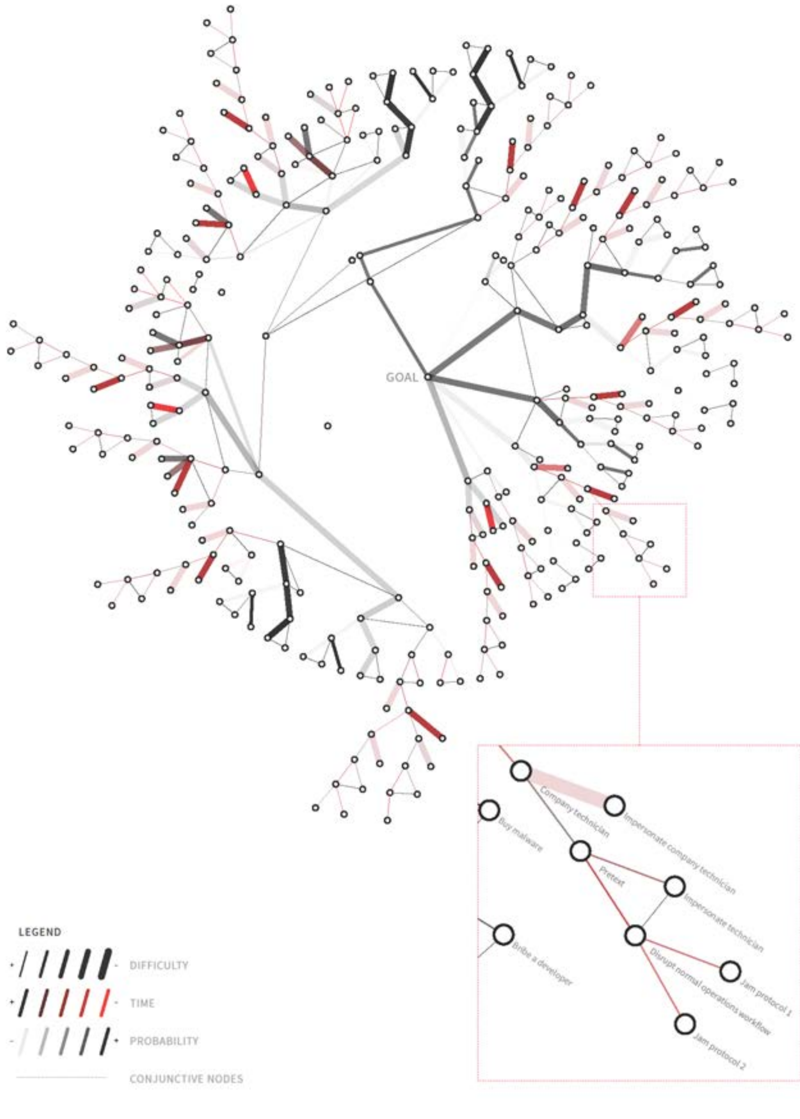
- Asked people in a shopping mall for email address, half of bank account number, data on online shopping
- Cues to cybercrime didn't reduce cases of revealing data
- Warning leaflet decreased revealing of emails addresses but not of bank account information or online shopping
- Differences due to changes in context, from a quiet office environment to a square in a shopping mall?
  - J-W. Bullée et al.: The persuasion and security awareness experiment: reducing the success of social engineering attacks

Visualize



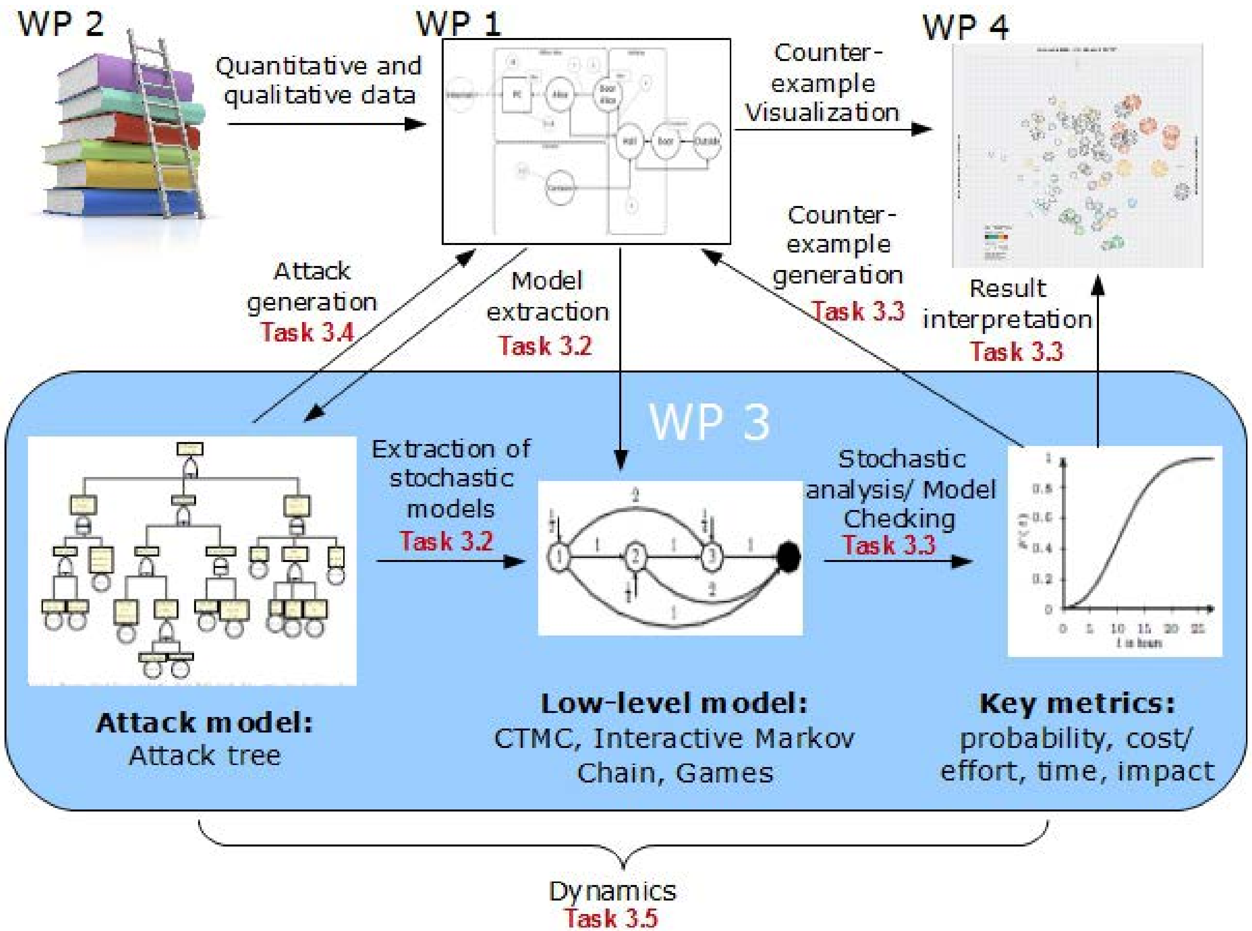
Visualise


CONJUNCTIVE NODES
CONJUNCTIVE NODE INSIDE A CONJUNCTIVE NODE


GOAL
LEGEND
DIFFICULTY
TIME
PROBABILITY
CONJUNCTIVE NODES
Company technician
Impersonate company technician
Buy malware
Pretext
Impersonate technician
Bribe a developer
Disrupt normal operations workflow
Jam protocol 1
Jam protocol 2

Conclusions

TRE$_S$PASS work flow

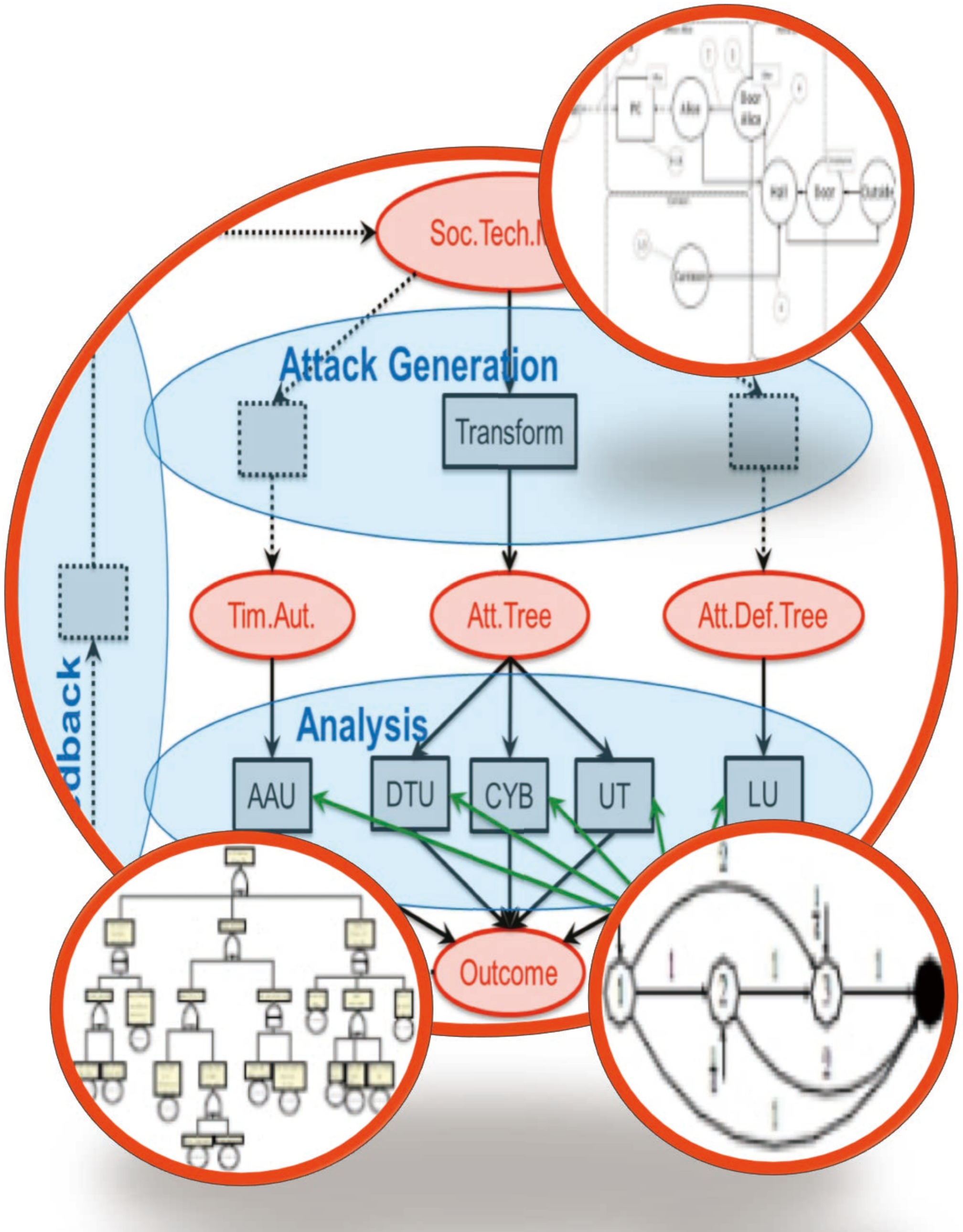


Innovation 1

- A **process methodology** to support risk analysis in socio-technical environments

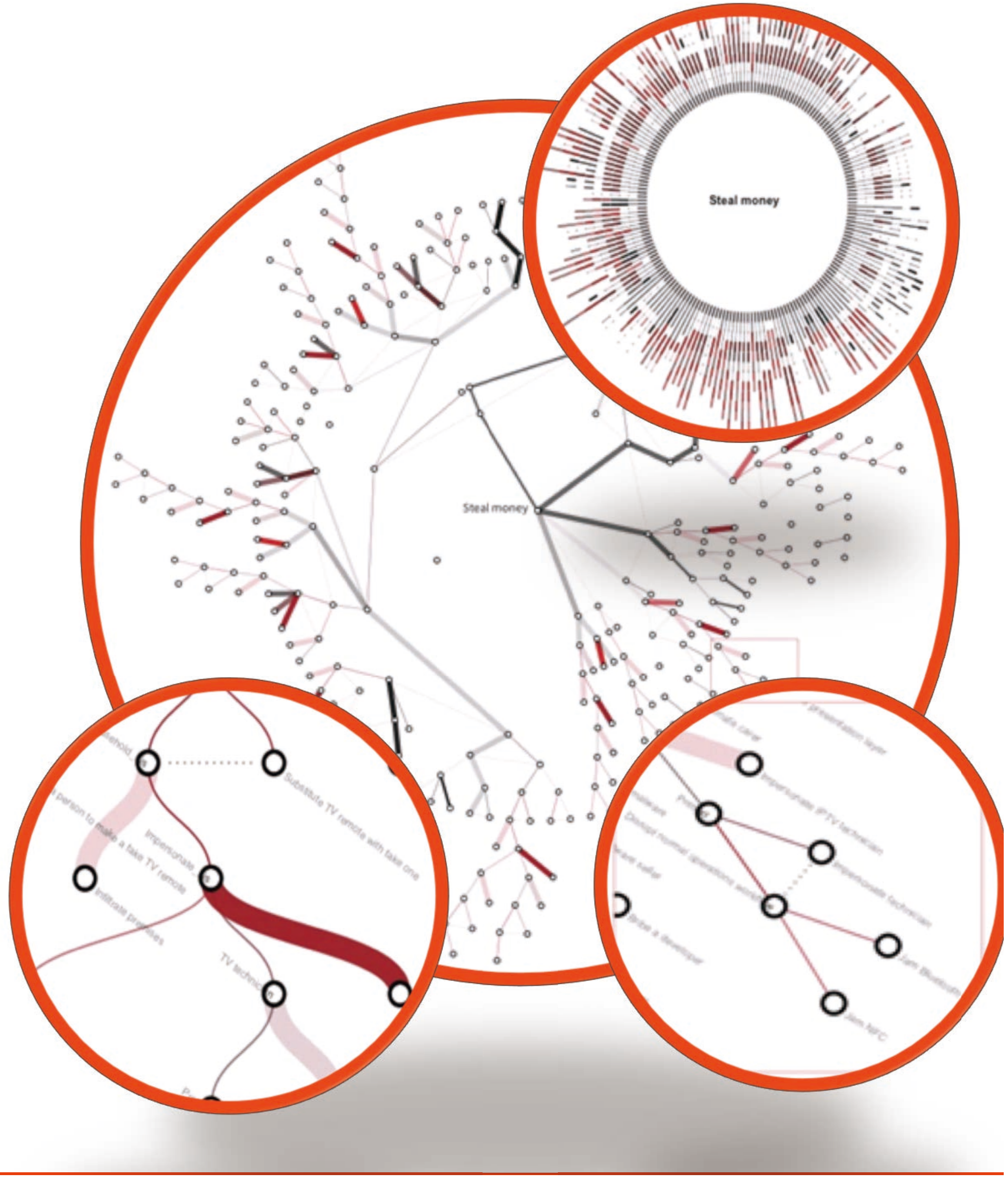
Innovation 2

- New and improved attack navigation **tools** to support these risk analyses of socio-technical attacks
- A portfolio of tools – not a single tool chain
- Many extensions of open source tooling



Innovation 3

- New **visualisation techniques** to enhance the presentation of complex socio-technical attacks
- Designed to :
  - Highlight important information
  - Better scalability



Summary

- TRE$_S$PASS includes human actors in its models
- Attack tress currently constructed manually, automatic generation under consideration
  - But would this be sufficient for capturing attacker's view?
- TRE$_S$PASS moves risk management from descriptive models to executable models
- Validation of methods in various case studies with industrial partners, more in the final project year

Next dissemination event

January 13-15, 2016	TREsPASS winter school on Security in Socio-Technical Systems

- Organizers: Christian W Probst, Rene Rydhof Hansen
- Technical University of Denmark, Campus Lyngby
- http://winterschool2015.trespass-project.eu/

Security by design is an oxymoron

- Core question: is data driven analysis right way forward?
  - TRE$_S$PASS started from this assumption but where can it get us?
- Is risk management about avoiding unforgivable vulnerabilities?
  - Automated tools are the way forward towards complete coverage of known attacks
- Is risk management about avoiding awkward surprises?
  - If you can predict something, it is no longer a surprise

Contact

predict
prioritise
prevent
TREsPASS

www.trespass-project.eu

contact@trespass-project.eu

Twitter: @TREsPASSProject

Contact us to join our public mailing list!

The research leading to these results has received funding from the European Union Seventh Framework Programme (FP7/2007-2013) under grant agreement n° 318003 (TREsPASS). This publication reflects only the author's views and the Union is not liable for any use that may be made of the information contained herein.

SEVENTH FRAMEWORK PROGRAMME

European Commission