Data Provenance and Attack Generation

predict
prioritise
prevent
TRESPASS

Christian W Probst
Technical University of Denmark

Advanced Data Collection and Risks Industry Workshop
2016/04/19

SEVENTH FRAMEWORK PROGRAMME

European Commission

Threat Scenario of Modern Organisations

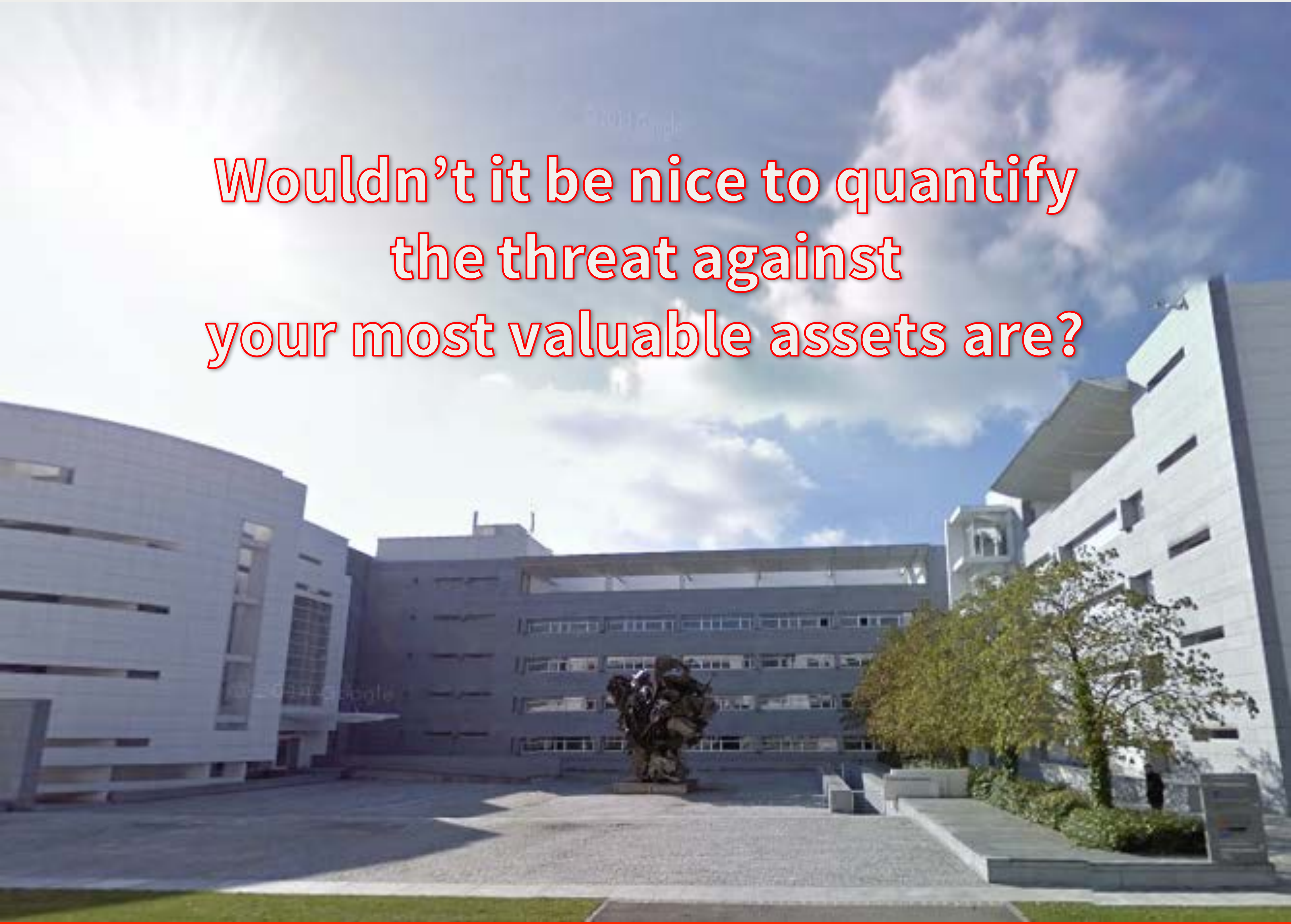
- Information security threats to organisations have changed completely over the last decade.

- New attacks cleverly exploit multiple organisational vulnerabilities, involving physical security and human behaviour.

- Defenders need to make rapid decisions regarding which attacks to block, as both infrastructure and attacker knowledge change rapidly.

Wouldn’t it be nice to know… how you can be attacked?

Wouldn’t it be nice to know
which paths an attacker might take
to your most valuable assets?



Wouldn’t it be nice to quantify
the threat against
your most valuable assets are?

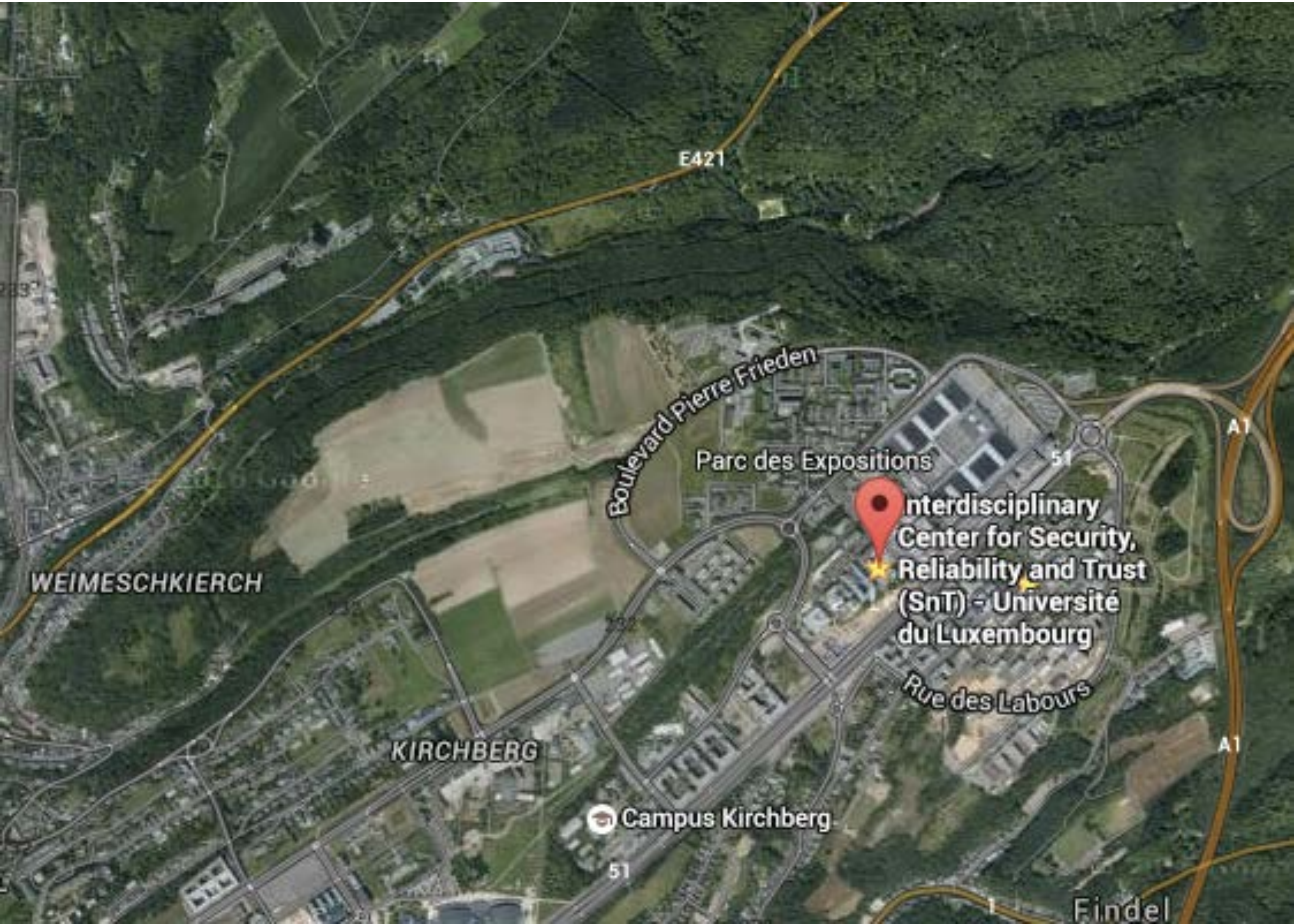
The TREsPASS Project

- Technology-supported Risk Estimation by Predictive Assessment of Socio-technical Security
- European FP7 integrated research project, 2012-2016
- 17 partners from academia and industry
- **Main result: "attack navigator" for identifying and ranking attacks on organisation**
- Analytic approach in contrast to today's methods.
- More at http://www.trespass-project.eu

The Attack Navigator

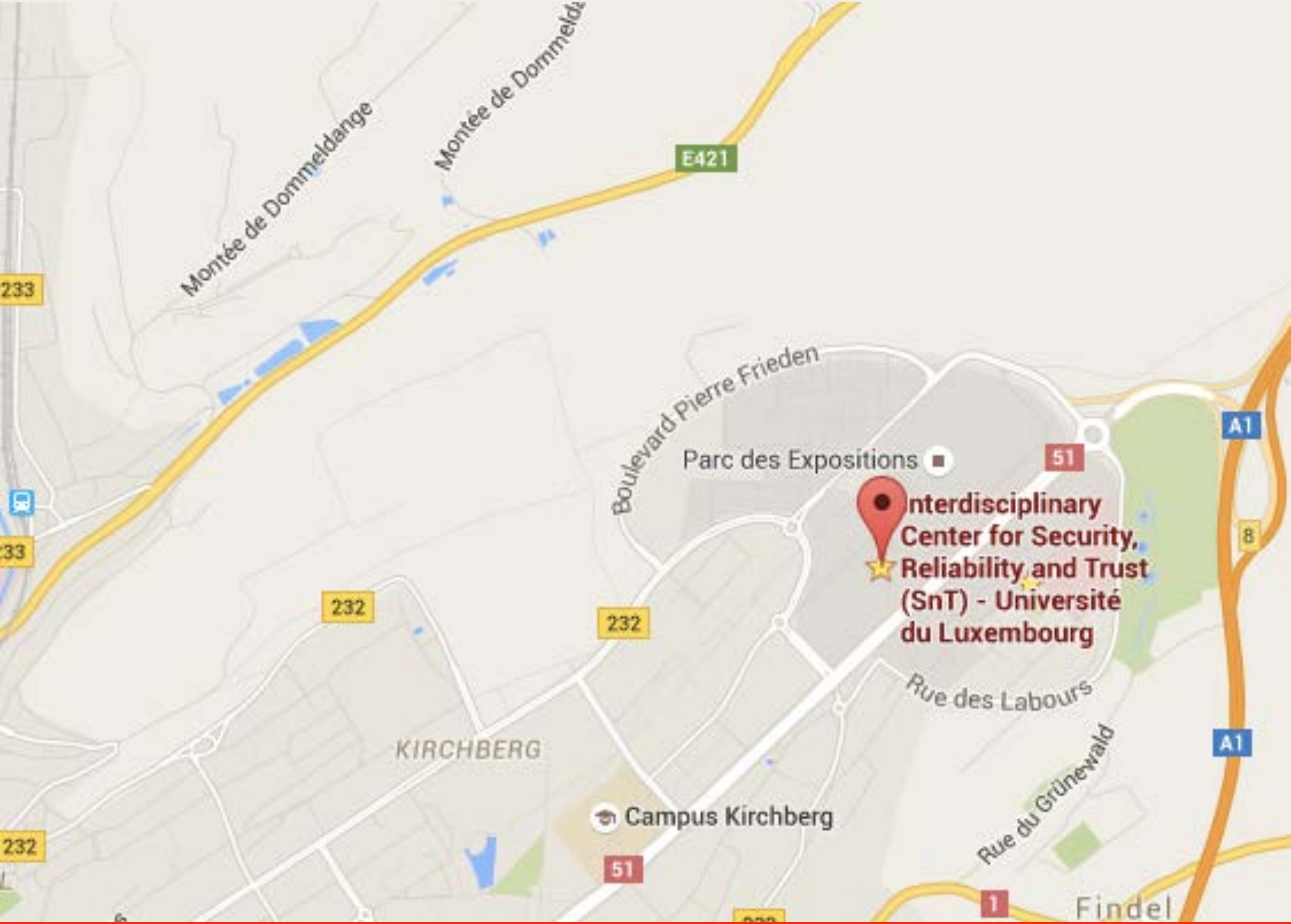
- **Attack navigator** identifies and ranks attacks on an organisation.
  - Supports prediction, prioritisation, and prevention of complex attack scenarios.
- Analytic risk assessment based on **system model of organisation** – infrastructure, policies, and employees.
- **Identifies all possible attacks** in the model!

Satellite View

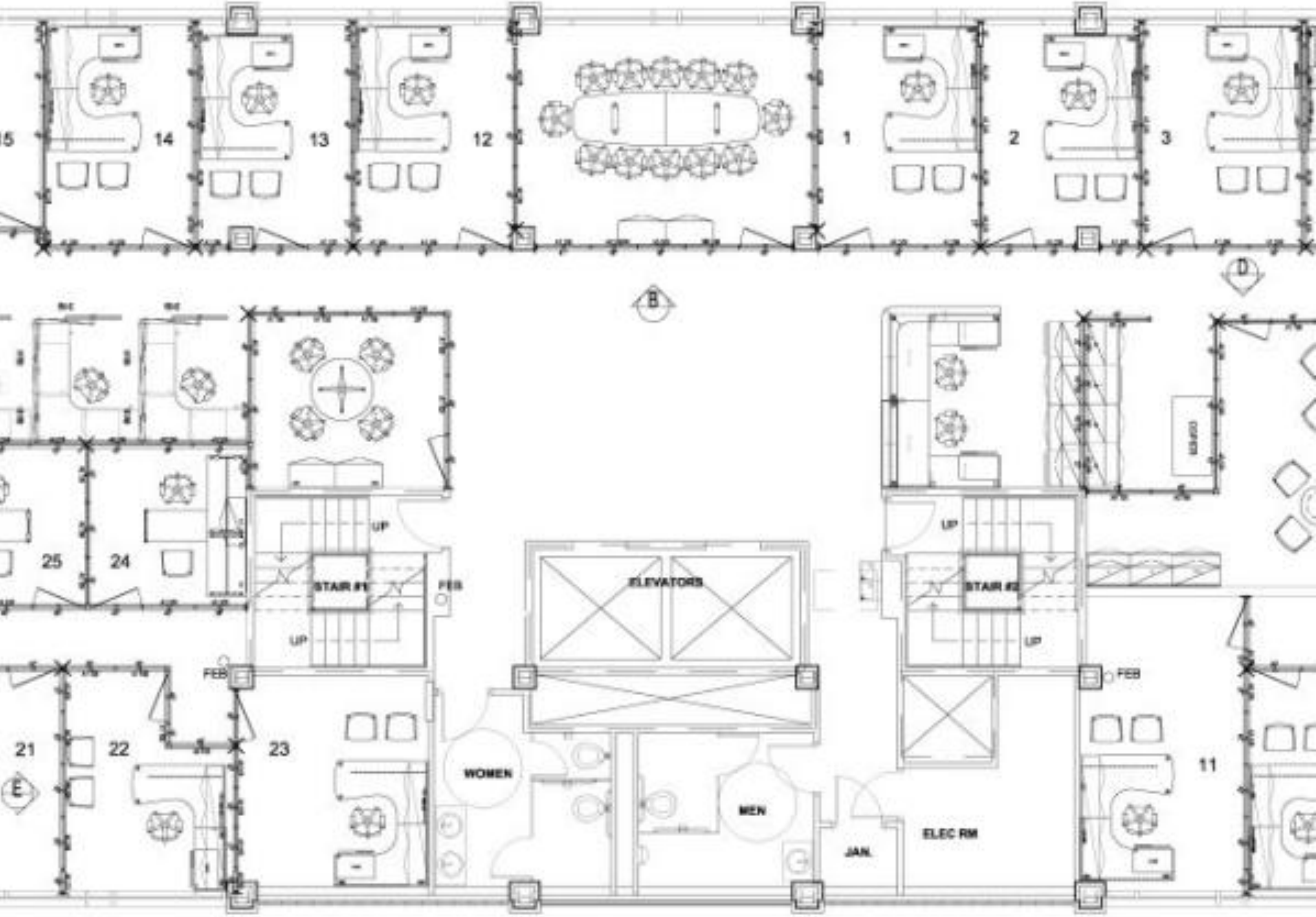


High Level View

Rue Jean Monnet
Interdisciplinary Center for Security, Reliability and Trust (SnT) - Université du Luxembourg
Max-Planck-Gesellschaft Zur Forderung Der Wissenschaften Ev
Banque Lblux Sa
Travail Kirchberg


Montée de Dommeldange
Montée de Dommeldange
E421
233
233
Boulevard Pierre Frieden
Parc des Expositions
51
Interdisciplinary Center for Security, Reliability and Trust (SnT) - Université du Luxembourg
A1
8
232
232
232
Rue des Labours
KIRCHBERG
A1
Rue du Grünewald
Campus Kirchberg
51
1
Findel

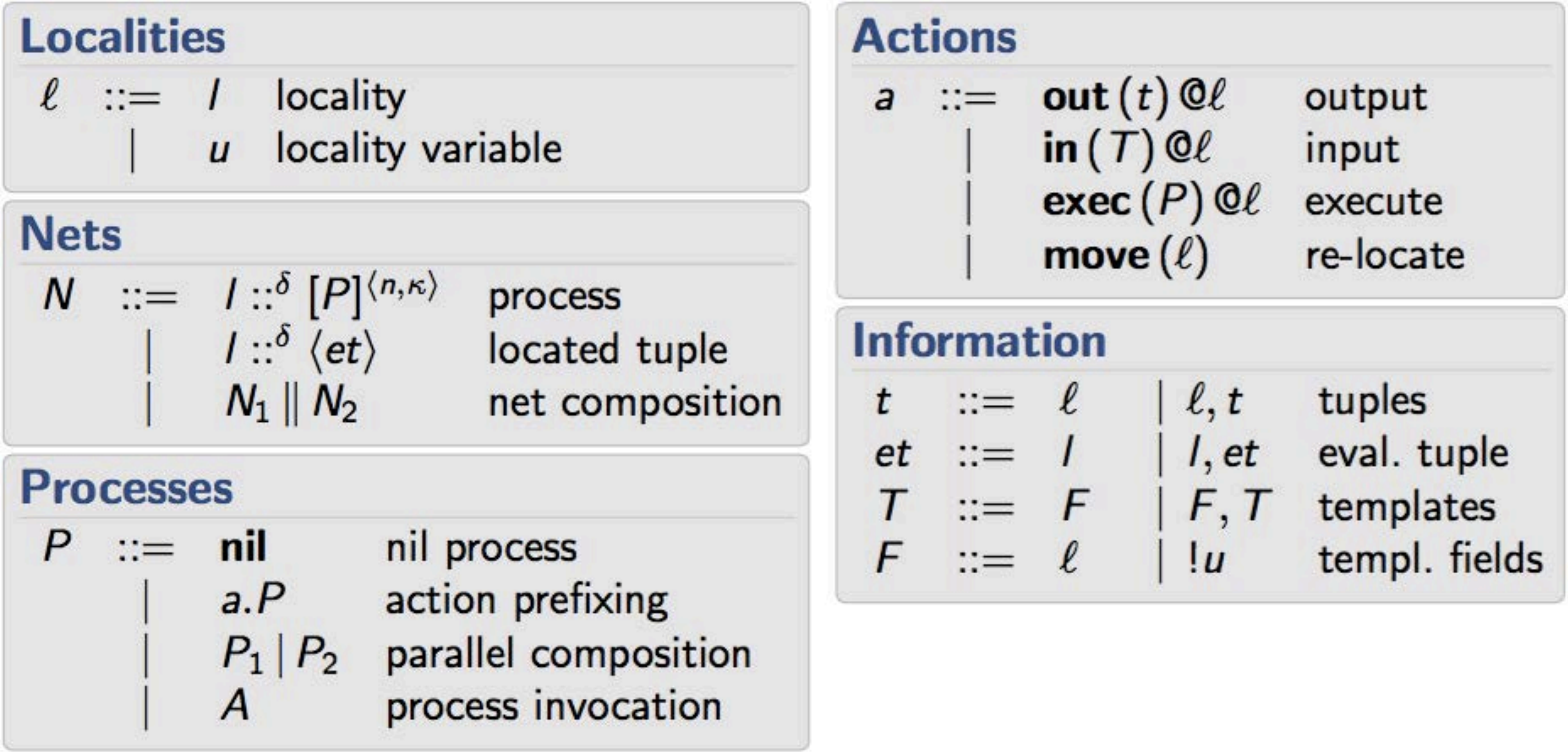
Model View


15
14
13
12
1
2
3
B
D
STAIR #1
UP
UP
FEB
ELEVATORS
STAIR #2
UP
UP
25
24
FEB
21
22
23
E
WOMEN
MEN
JAN.
ELEC RM
FEB
11

Our System Model

- Map of the attack navigator
- Models real-world systems – physical, virtual, social layer!
  - Relevant properties/actions
  - Maps to an analysable formalism
  - Apply static analyses and model checking
- System Model
  - Directed graph
  - Models all locations that can be accessed/store data
  - Models all entities that can move in the system

Socio-Technical Modelling Language



Localities

ℓ	$::=$	l	locality
	$\mid$	u	locality variable

Nets

N	$::=$	$l ::^{\delta} [P]^{\langle n,\kappa \rangle}$	process
	$\mid$	$l ::^{\delta} \langle et \rangle$	located tuple
	$\mid$	$N_1 \parallel N_2$	net composition

Processes

P	$::=$	**nil**	nil process
	$\mid$	$a.P$	action prefixing
	$\mid$	$P_1 \mid P_2$	parallel composition
	$\mid$	A	process invocation

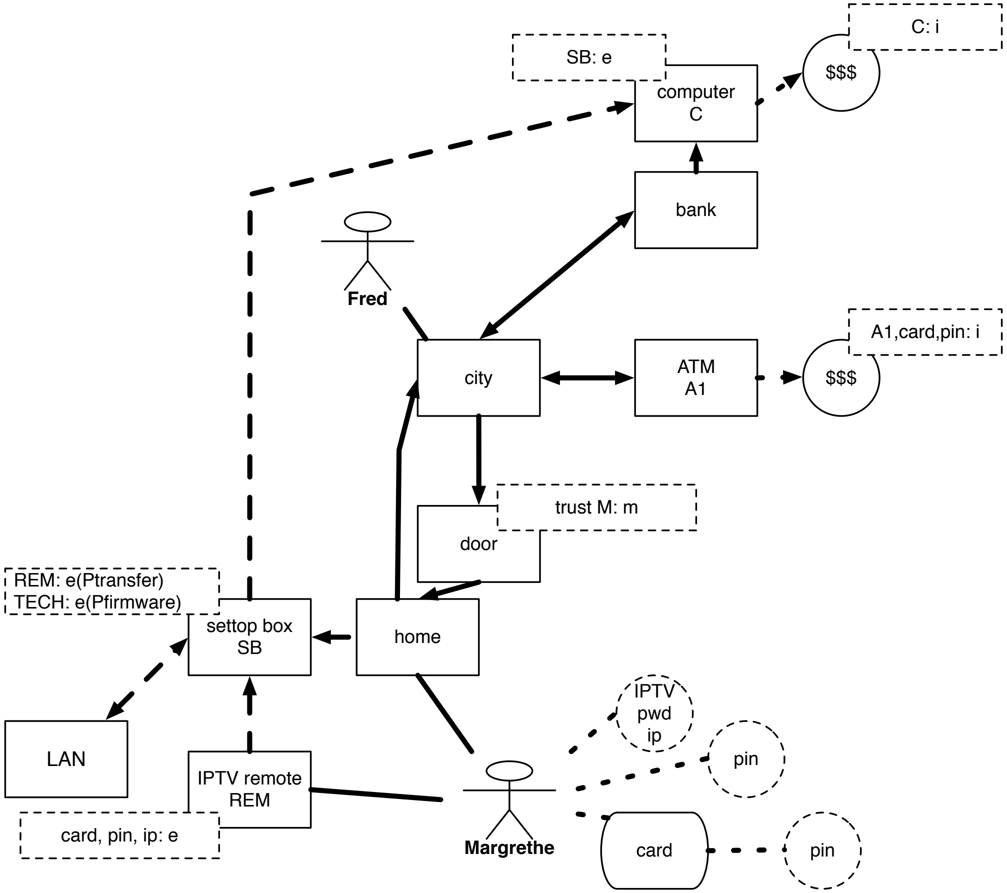
Actions

a	$::=$	$\mathbf{out}\,(t)\,@\ell$	output
	$\mid$	$\mathbf{in}\,(T)\,@\ell$	input
	$\mid$	$\mathbf{exec}\,(P)\,@\ell$	execute
	$\mid$	$\mathbf{move}\,(\ell)$	re-locate

Information

t	$::=$	ℓ	$\mid$	ℓ, t	tuples
et	$::=$	l	$\mid$	l, et	eval. tuple
T	$::=$	F	$\mid$	F, T	templates
F	$::=$	ℓ	$\mid$	$!u$	templ. fields

Example Model

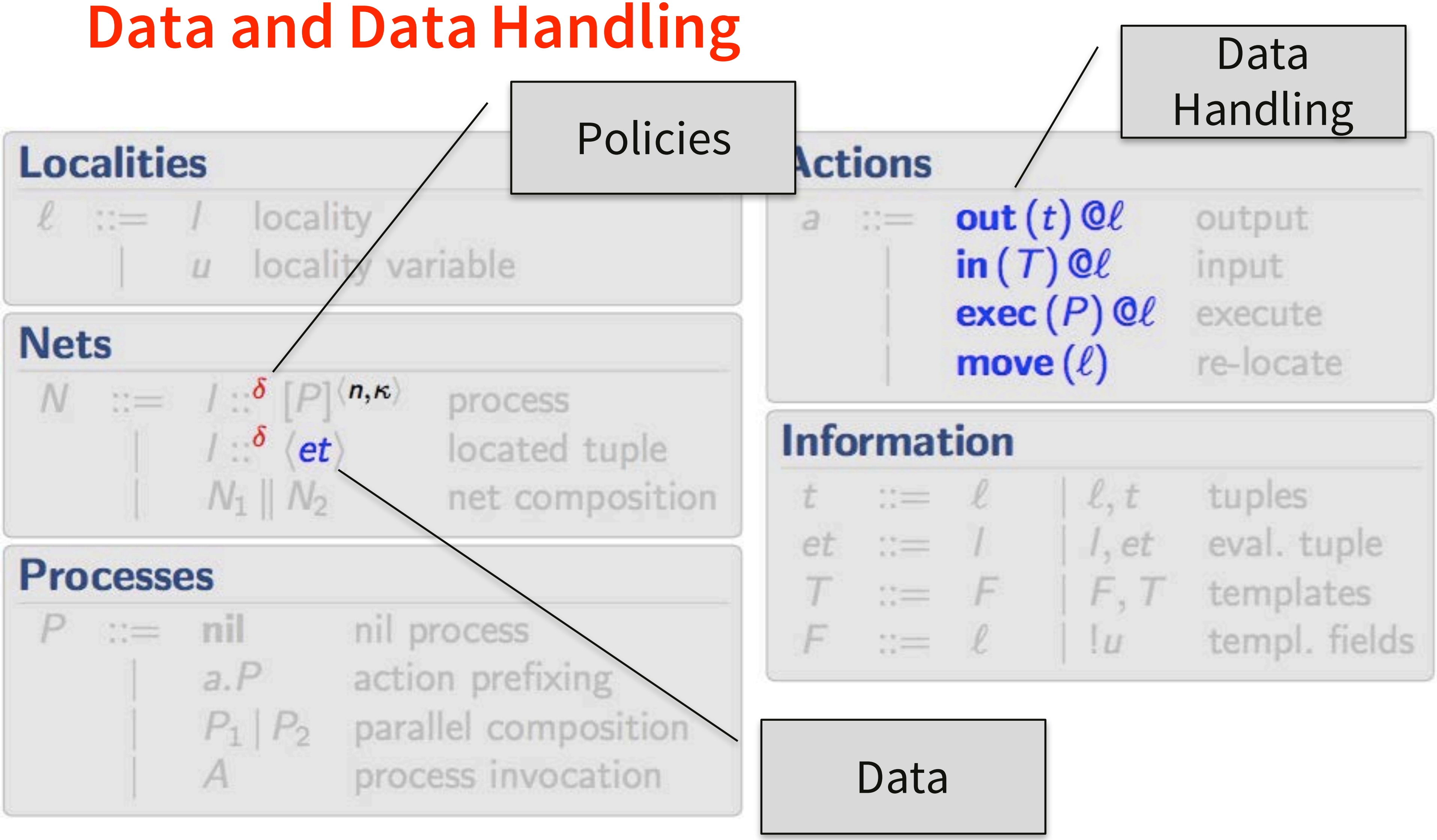


What are “valuable” assets?

- The modelled organisation decides, which elements are important
  - Virtual or physical assets,
  - Operational goals, or
  - Global policies.
- Assets can be accessed by actors or processes, and
- Can move/be moved around the system!

➢ **This blurred location results in additional challenges!**

Data and Data Handling



Policies

Data Handling

Data

Localities

ℓ	$::=$	l	locality
	$\mid$	u	locality variable

Nets

N	$::=$	$l ::^{\delta} [P]^{\langle n,\kappa \rangle}$	process
	$\mid$	$l ::^{\delta} \langle et \rangle$	located tuple
	$\mid$	$N_1 \parallel N_2$	net composition

Processes

P	$::=$	**nil**	nil process
	$\mid$	$a.P$	action prefixing
	$\mid$	$P_1 \mid P_2$	parallel composition
	$\mid$	A	process invocation

Actions

a	$::=$	**out** (t) @ℓ	output
	$\mid$	**in** (T) @ℓ	input
	$\mid$	**exec** (P) @ℓ	execute
	$\mid$	**move** (ℓ)	re-locate

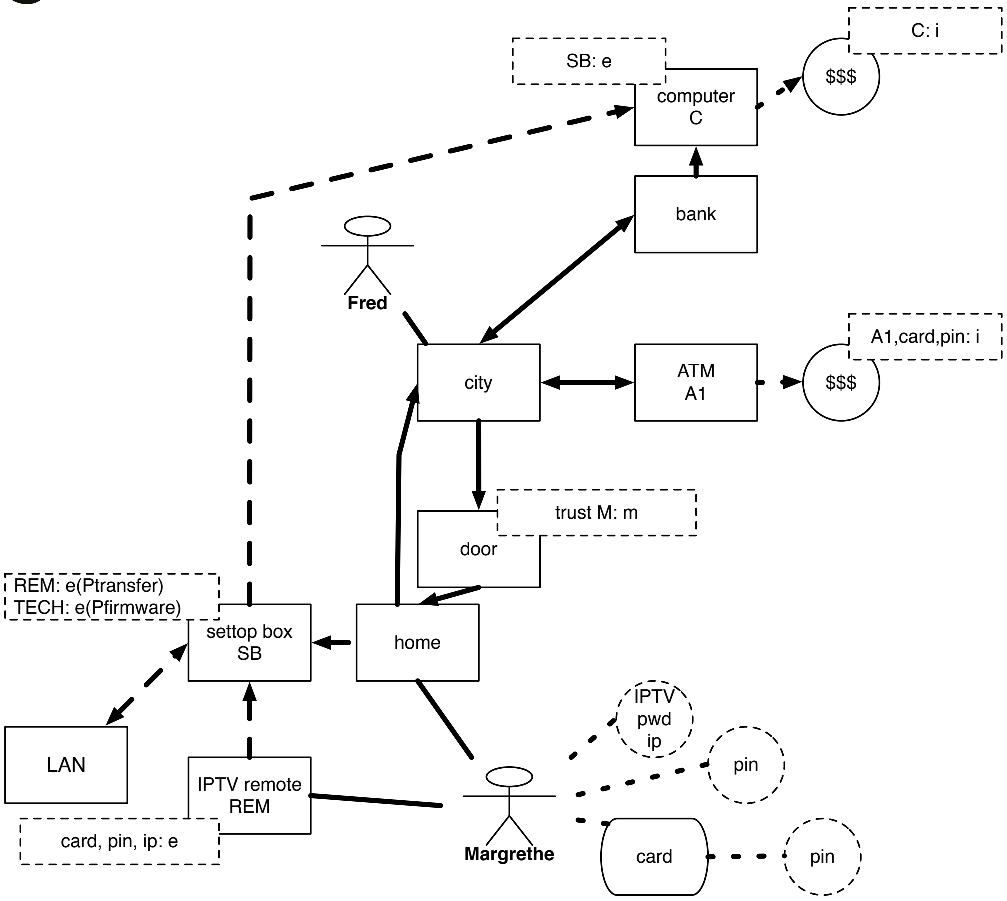
Information

t	$::=$	ℓ	$\mid$	ℓ, t	tuples
et	$::=$	l	$\mid$	l, et	eval. tuple
T	$::=$	F	$\mid$	F, T	templates
F	$::=$	ℓ	$\mid$	$!u$	templ. fields

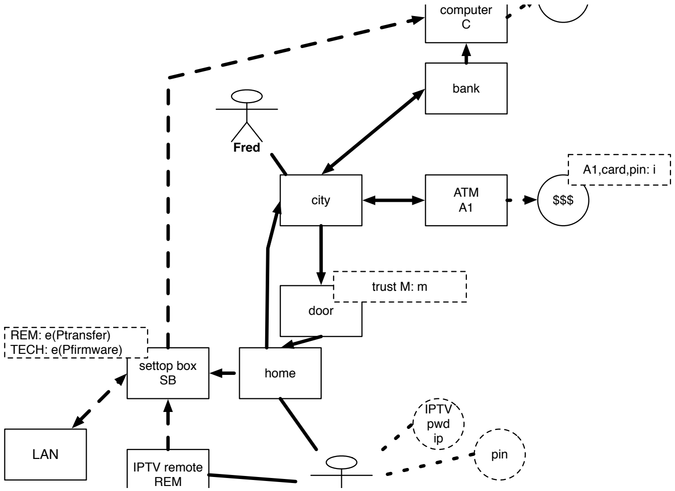
Systematic generation of attacks from TRE$_S$PASS models

Goal: use M’s card to get $$$;

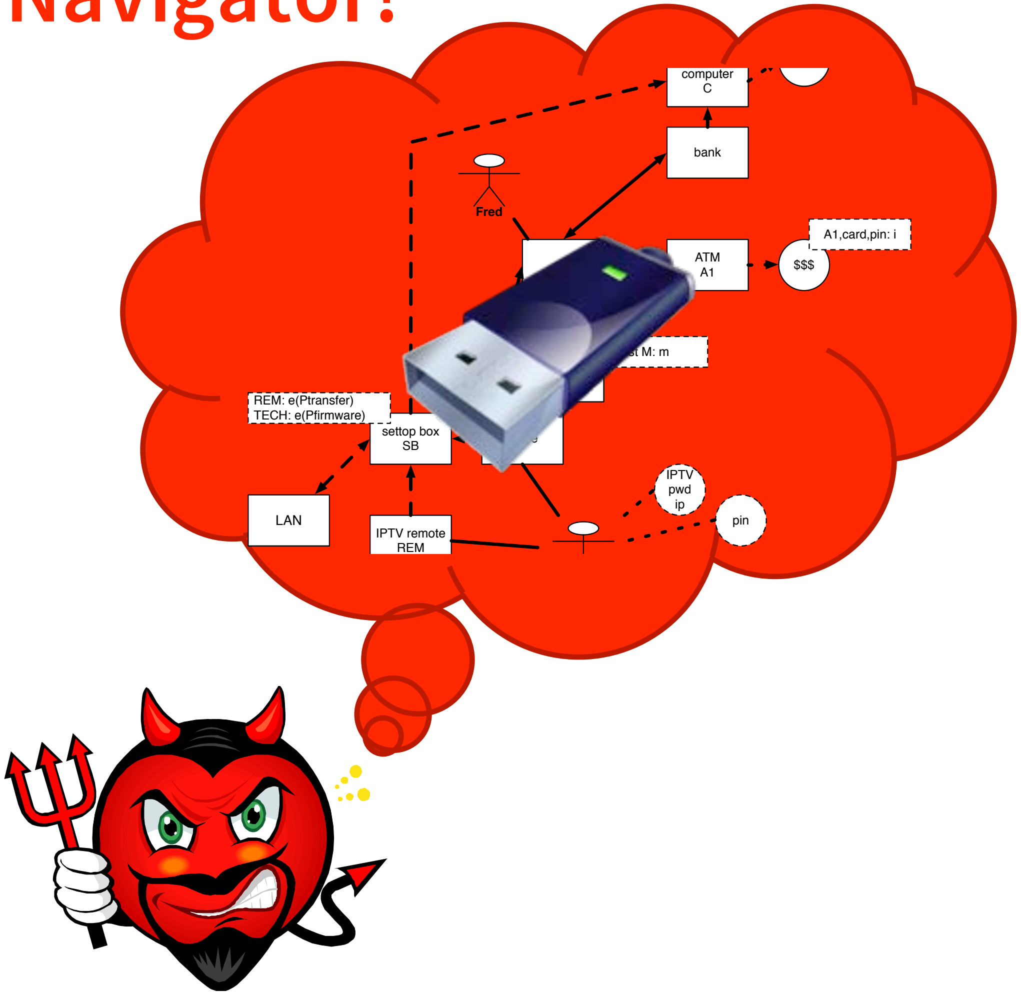
- Defender specifies undesirable states of the organisation – **the destinations of an attacker!**
- Attack navigator identifies all possible ways of reaching that states – **the routes of an attacker!**

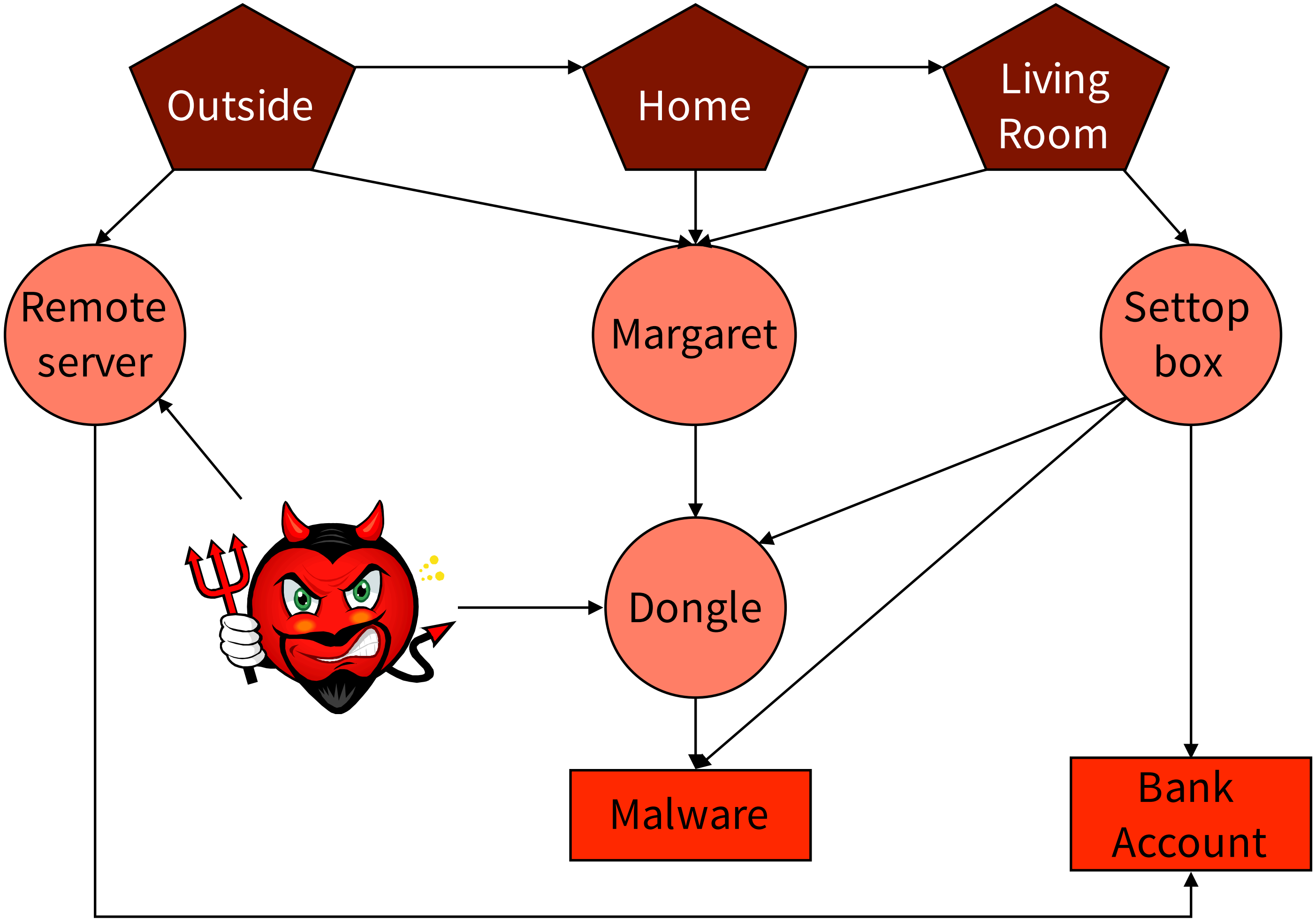


How do I get the money?



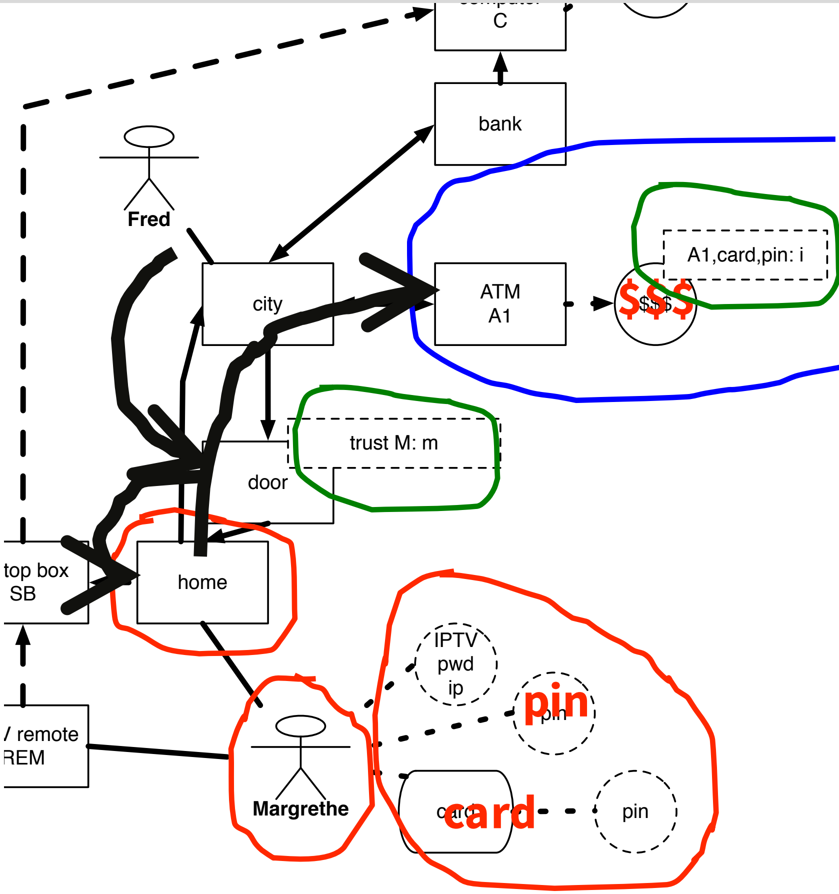
Ask the TRESPASS Attack Navigator!

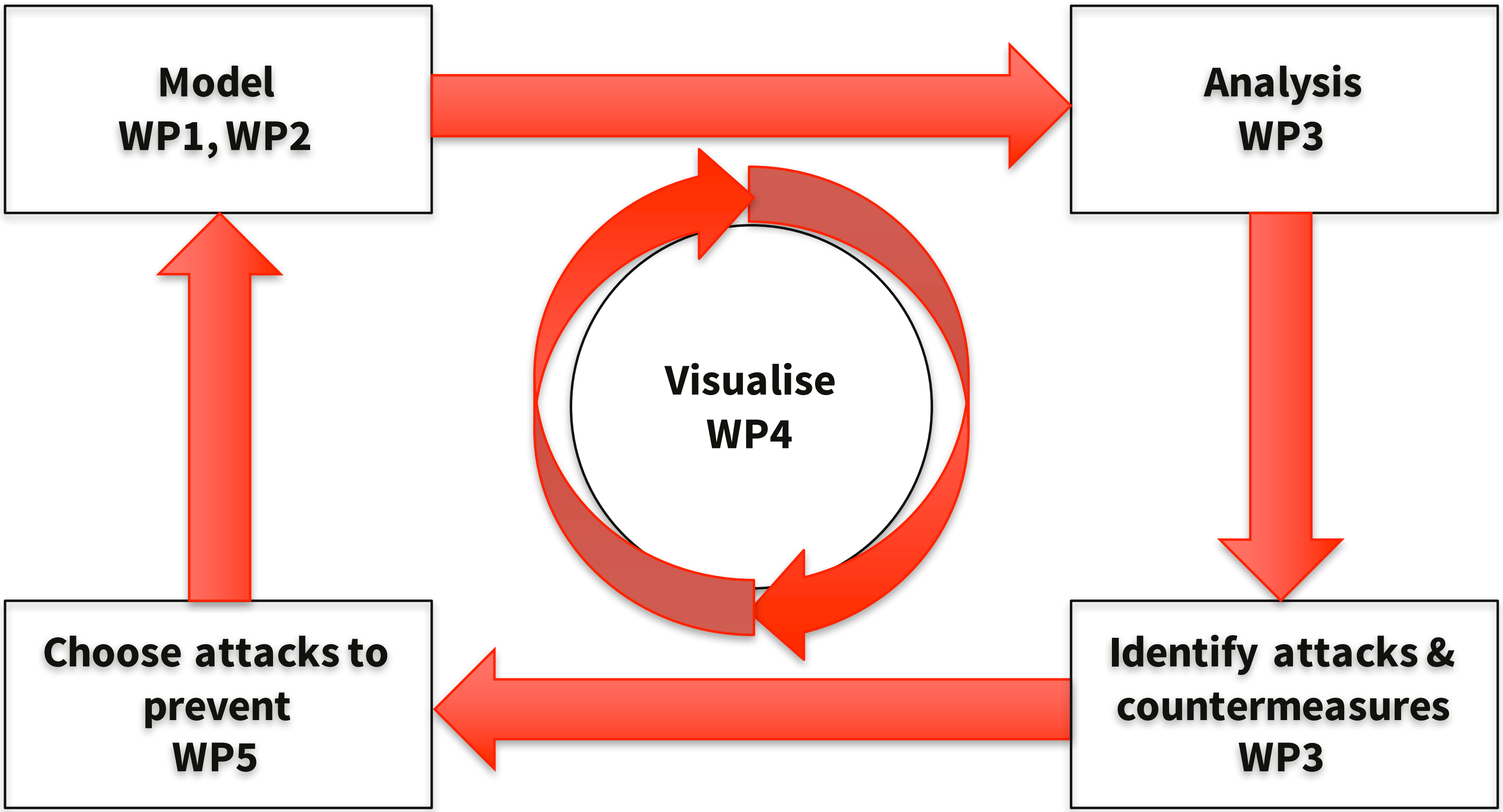



Outside
Home
Living Room
Remote server
Margaret
Settop box
Dongle
Malware
Bank Account

Goal: use M’s card to get $$$;

- This is a **navigator map** and the **identified routes**!
- Specify what to protect – the attack navigator shows you how that will fail (in your model).




Model
WP1, WP2
Analysis
WP3
Visualise
WP4
Identify attacks & countermeasures
WP3
Choose attacks to prevent
WP5

Data Provenance

- To protect data (or assets) we need to identify where it can go or moved!
  - If the list of people having saved unreported income in Liechtenstein is well protected in the safe – who cares!
  - If it quickly can be photographed and taken out of the premises – now that’s interesting. Or not.
- Policies regulate access to data and guide the identification of areas that can be ”reached” by data
- This is very similar to tainting and white box testing!
  - The model “knows” everything about the modelled system, and tainting allows to test where data will be able to go.

Data Targets and Provenance

- **Data Targets** are potential targets for data items
  - Forward analysis
  - User inputs data at PC1, moves through FR
  - User starts process at PC2, inputs data, moves through FR
- **Data Provenance** identifies where data may come from
  - Backward analysis
  - Data at WWW was output by process at PC2, process was started by U, input data at PC1
  - User U has brought process inside the organisation, or User U has received process by email or download

Data Access and Handling

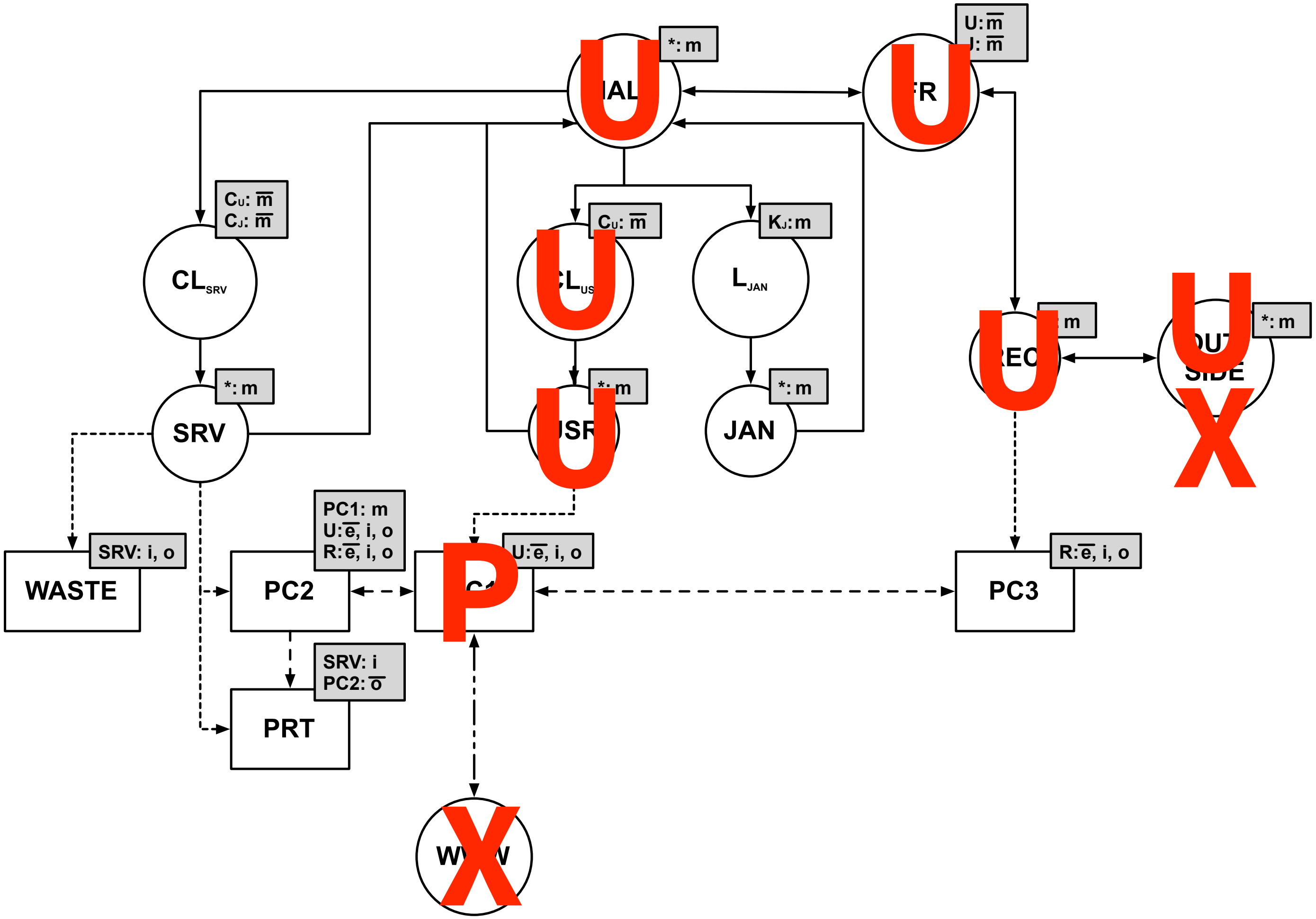
- Policies require actions on assets and by actors and processes.
- Performing entity must have some credentials to be allowed to perform an action.
  - Data access through actors and processes.
  - Spawning of processes.
  - Movement through the system.

- Identify potential data flow
- Trace which actors/processes can access the data
- Trace which policies influence the data flow
- Based on policies and connectivity

Generating Attacks based on Data Locations

- Now we move **from considering attackers** whom we cannot control and their potential, unpredictable movements and actions,
- **To considering the data** that we can control, and its movement in the organisation.
  - ”Simple” reachability analysis!
  - Backtracking from undesired state through actions causing the system to reach that state.
  - “Reverse engineering” security.

Policy: Data of type "X" may never leave the organisation

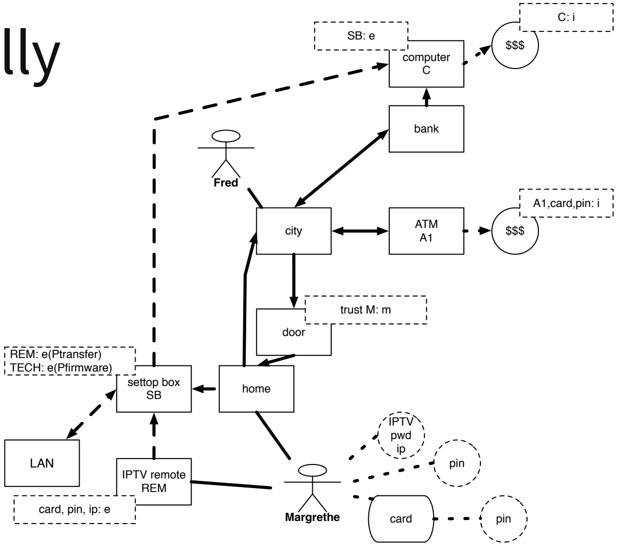


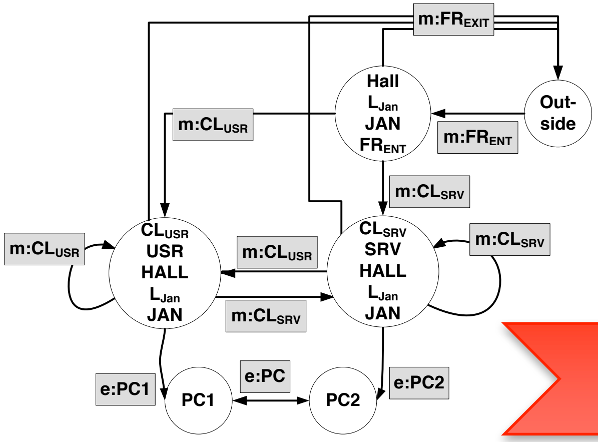
Data Provenance and Attack Generation

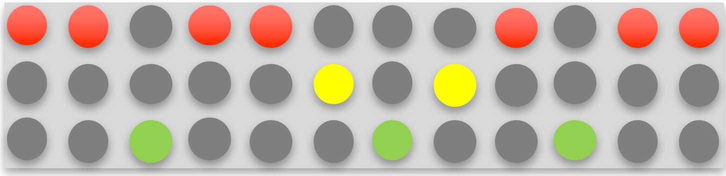
- Attack generation must be dynamic to account for “moving” data.
- Needed to address insiders, data in cloud infrastructures, or bring-your-own-device scenarios.
- Orthogonal to the “normal” actor-centric view of organisational security.

Security Dashboard for Socio-Technical Systems

- Based on identified risks.
- Generate surveillance mechanism based on possible attacks.
- Tracks observable movements of actors **and** data (logged manually or automatically).







predict
prioritise
prevent
TREsPASS

Contact

www.trespass-project.eu

contact@trespass-project.eu

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