Ontological Foundations for Vulnerability Analysis of Security Policies

Karolina Bataityte[1] Dr. Vassil Vassilev[2] Dr.Olivia Jo Gill[1]

[1]School of Computing and Digital Media,
London Metropolitan University,
London, UK

[2]Cyber Security Research Centre,
London Metropolitan University,
London, UK

Seminar, 2020 January

{k.bataityte,v.vassilev,o.gill}@londonmet.ac.uk

LONDON METROPOLITAN UNIVERSITY

Outline

Introduction

- Logical vulnerability- breaking into the system by manipulating rules of the system and security.
- We want to analyse logical vulnerabilities by validating the security policies throughout the journey.
- Theoretical motivation: to model dynamics using static representation.

Methodology

Definition

A model $M = (T, R, G)$ where T is a $\mathcal{ALC}$ TBox T containing all terminological axioms and R is a set of SWRL rules and G is a directed graph.

Figure: Multi- level Model for Analysis

Lets start: Ontological Level

The term ontology in narrow logical sense provides the terminology, which can be used for building the domain model, together with its interpretation in the semantic domain [4].

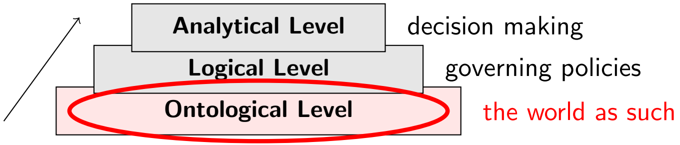


Figure: Multi- level Model for Analysis

Logical Foundations: Description Logic $\mathcal{ALC}$

The interpretation I is a pair $I = (\triangle^I, \cdot^I)$, where $\triangle^I$ is a non-empty set (domain) and $\cdot^I$ is a mapping function [5].

Concepts		Roles	
Syntax	Semantics	Syntax	Semantics
$\top$	$\triangle^I$	R	$R^I \subseteq \triangle^I \times \triangle^I$
$\bot$	$\emptyset$	$Domain(R, C)$	$< a, b > \in R^I \rightarrow a \in C^I$
A	$A^I \subseteq \triangle^I$	$Range(R, C)$	$< a, b > \in R^I \rightarrow b \in C^I$
$\neg C$	$\triangle^I \backslash C^I$		
$C \sqcap D$	$C^I \cap D^I$		
$C \sqcup D$	$C^I \cup D^I$		
$\forall R.C$	$\{a \in \triangle^I \vert \forall b.(< a, b > \in R^I \rightarrow b \in C^I)\}$		
$\exists R.C$	$\{a \in \triangle^I \vert \exists b.(< a, b > \in R^I \wedge b \in C^I)\}$		
where C, D are concepts, A is an atomic concept, R is a role.			

Given interpretation I in M of axiom α, we say that M is a model of α under I if M satisfies α, written $I \models \alpha$. We will be expressing the domain restrictions as $\exists R.\top \sqsubseteq C$ and the range restrictions as $\top \sqsubseteq \forall R.C$ [6].

LONDON METROPOLITAN UNIVERSITY

Ontology of the Domain

- We split the semantic domain $\triangle$ (a non-empty set) into three disjoint subdomains:
  - Subdomain of Entities as $\triangle_{Entities}$,
  - Subdomain of Events as $\triangle_{Events}$,
  - Subdomain of Situations as $\triangle_{Situations}$.
- The interpretation of $\mathcal{ALC}$ concepts and roles in the domain are as follows:
  - $\mathrm{Entity}^{\mathrm{I}} \subseteq \triangle^{I}_{Entities}$,
  - $\mathrm{Event}^{\mathrm{I}} \subseteq \triangle^{I}_{Events}$,
  - $\mathrm{Situation}^{\mathrm{I}} \subseteq \triangle^{I}_{Situations}$.
  - $\mathrm{Action}^{\mathrm{I}} \subseteq \triangle^{I}_{Situations} \times \triangle^{I}_{Situations}$
- The ontology can have as many *named concepts* and *named roles*.
  - $\mathrm{Entity}_{\mathrm{x}}$, $\mathrm{Situation}_{\mathrm{y}}$, $\mathrm{Event}_{\mathrm{z}}$, etc.

$$Situation \sqcap Event \sqsubseteq \perp, Situation \sqcap Entity \sqsubseteq \perp, Entity \sqcap Event \sqsubseteq \perp. \quad (1)$$

Static Model of the World

Term	DL Category	Use in modelling
Situation	concept	partial static description of the world
Event	concept	asynchronous activity
Entity	concept	qualitative descriptor
Action	role	synchronous activity
occur–in	role	event occurrence
present–at	role	situation description
part–of	role	event description
describe	role	describing entities quantitatively or specifying qualitative dependencies
chain	role	connecting events causally

Table: Vocabulary of the Domain Ontology

LONDON METROPOLITAN UNIVERSITY

Static Model of the World

Domain and Range axioms:

$$\exists Action.\top \sqsubseteq Situation, \top \sqsubseteq \forall Action.Situation \tag{2}$$

$$\exists chain.\top \sqsubseteq Event, \top \sqsubseteq \forall chain.Event \tag{3}$$

$$\exists occur{-}in.\top \sqsubseteq Event, \top \sqsubseteq \forall occur{-}in.Situation \tag{4}$$

$$\exists part{-}of.\top \sqsubseteq Entity, \top \sqsubseteq \forall part{-}of.Event \tag{5}$$

$$\exists present{-}at.\top \sqsubseteq Entity, \top \sqsubseteq \forall present{-}at.Situation \tag{6}$$

$$\exists describe.\top \sqsubseteq Entity, \top \sqsubseteq \forall describe.Entity \tag{7}$$

$$Entity \xrightarrow{part{-}of} Event$$

Illiustration

If we have TBox T with situations and entities as follows:

$$T := \{\mathrm{Entity_x} \sqsubseteq \mathit{Entity}, \mathrm{Situation_y} \sqsubseteq \mathit{Situation}\} \tag{8}$$

then each description of the $\mathrm{Situation_y}$ using the entities can extend it as follows:

$$T' := T \cup \{\mathrm{Entity_x} \sqsubseteq \exists \mathit{present{-}at}.\mathrm{Situation_y}\}. \tag{9}$$

Example

Let's consider the situation *LoggedIn* and the entity *User*. For this scenario the TBox T is

$$T := \{\mathit{User} \sqsubseteq \mathit{Entity}, \mathit{LoggedIn} \sqsubseteq \mathit{Situation},$$

$$\mathit{User} \sqsubseteq \exists \mathit{present{-}at}.\mathit{LoggedIn}\}$$

Graphical Representation

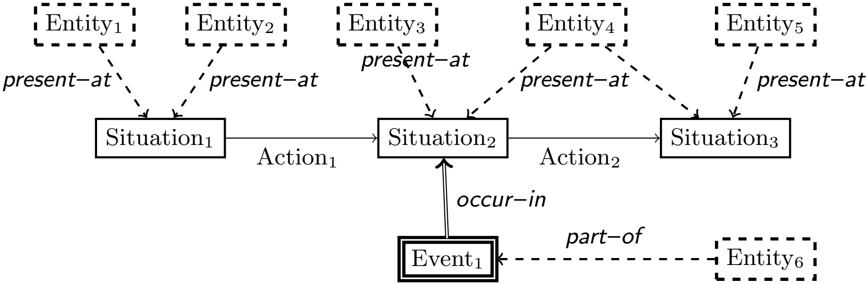


Figure: A graphical representation of two-step journey

World Dynamics

Definition

A GBox G is a set of pairs of actions and entities, representing the action parameters $G = \{\langle entity_y, Action_z \rangle, \langle Action_z, entity_y \rangle\}$ where pair $\langle entity_y, action_z \rangle$ is for input parameters and pair $\langle Action_z, entity_y \rangle$ is for output parameters.

World Dynamics: Input Paramters

In order for an entity to be an input parameter, it must meet the following:

1. $\mathrm{Entity_e} \sqsubseteq \exists \mathit{present{-}at}.\mathrm{Situation_x}$,
2. $\exists \mathrm{Action_z}.\top \sqsubseteq \mathrm{Situation_x}$.

If both conditions hold, we can say GBox $G = \{\langle \mathrm{Entity_e}, \mathrm{Action_z} \rangle\}$. It can be formalized as the following axiom:

$$\mathrm{Entity_e} \sqsubseteq \exists \mathit{present{-}at}.(\mathrm{Situation_x} \sqcap \exists \mathrm{Action_z}.\top) \tag{10}$$

which says that $\mathrm{Entity_e}$ is connected to a $\mathrm{Situation_x}$ via *present–at* and there is an $\mathrm{Action_z}$ starting at $\mathit{Situation_x}$ and leading to another unknown *Situation*.

$$\mathrm{Entity_e} \xrightarrow{\mathit{present{-}at}} \mathrm{Situation_x} \xrightarrow{\mathrm{Action_z}} \top$$

World Dynamics: Output Paramters

In order for an entity to be an output parameter, it must meet the following:

1. $\mathrm{Entity_e} \sqsubseteq \exists \textit{present–at}.\mathrm{Situation_y}$,
2. $\top \sqsubseteq \forall \mathrm{Action_z}.\mathrm{Situation_y}$.

If both conditions hold, we can say GBox $G = \{\langle \mathrm{Action_z}, \mathrm{Entity_e} \rangle\}$. It can be formalized as follows:

$$\mathrm{Entity_e} \sqsubseteq \exists \textit{present–at}.\exists \mathrm{Action_z}.\mathrm{Situation_y} \tag{11}$$

which says that *Entity*$_e$ describes *Situation*$_y$ via *present–at* and *Action*$_z$ leads to *Situation*$_y$ after it executes.

$$\mathrm{Entity_e} \xrightarrow{\textit{present–at}} \cdot \xrightarrow{\mathrm{Action_z}} \mathrm{Situation_y}$$

World Dynamics

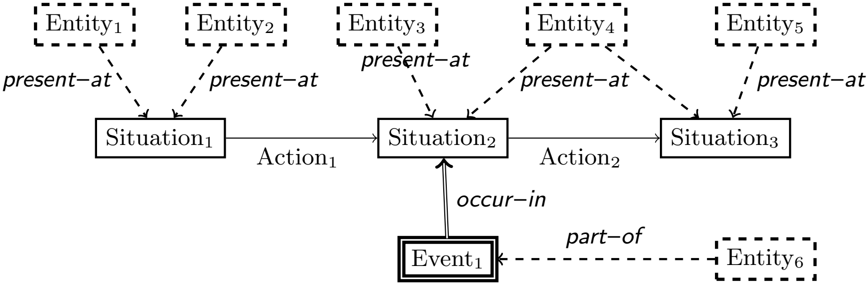


Figure: A graphical representation of two-step journey

Next: Logical Level

Logical level captures contrains, dependencies, descriptive completion and domain rules.

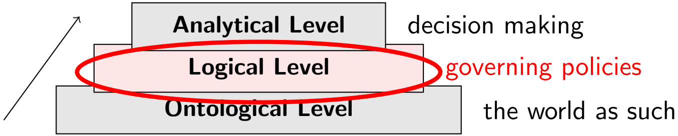


Figure: Multi- level Model for Analysis

Entity Triangulation

Proposition 1 (Entity Triangulation). Let the following TBox T be given:

$$T := \{Entity \sqsubseteq \exists part\text{–}of.Event, \tag{12a}$$

$$Event \sqsubseteq \exists occur\text{–}in.Situation\} \tag{12b}$$

Then the following holds:

$$T' := T \cup \{Entity \sqsubseteq \exists present\text{–}at.Situation\}. \tag{13}$$

$$\boxed{Entity} \xrightarrow{\quad part\text{–}of \quad} \boxed{Event}$$

Entity Triangulation

Proposition 1 (Entity Triangulation). Let the following TBox T be given:

$$T := \{Entity \sqsubseteq \exists part\text{–}of.Event, \tag{12a}$$

$$Event \sqsubseteq \exists occur\text{–}in.Situation\} \tag{12b}$$

Then the following holds:

$$T' := T \cup \{Entity \sqsubseteq \exists present\text{–}at.Situation\}. \tag{13}$$

$$\boxed{Entity} \xrightarrow{part\text{–}of} \boxed{Event} \xrightarrow{occur\text{–}in} \boxed{Situation}$$

Entity Triangulation

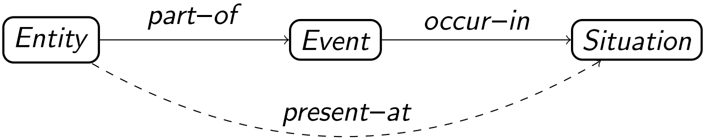
Proposition 1 (Entity Triangulation). Let the following TBox T be given:

$$T := \{\mathit{Entity} \sqsubseteq \exists \mathit{part{-}of}.\mathit{Event}, \tag{12a}$$

$$\mathit{Event} \sqsubseteq \exists \mathit{occur{-}in}.\mathit{Situation}\} \tag{12b}$$

Then the following holds:

$$T' := T \cup \{\mathit{Entity} \sqsubseteq \exists \mathit{present{-}at}.\mathit{Situation}\}. \tag{13}$$



Entity Transitivity

Proposition 2 (Entity Transitivity). Let the following TBox T be given:

$$T := \{\mathrm{Entity_y} \sqsubseteq \exists \mathit{describe}.\mathrm{Entity_x}, \tag{14a}$$

$$\mathrm{Entity_x} \sqsubseteq \exists \mathit{present\text{–}at}.\mathrm{Situation_x}\} \tag{14b}$$

Then the following holds:

$$T' := T \cup \{\mathrm{Entity_y} \sqsubseteq \exists \mathit{present\text{–}at}.\mathrm{Situation_x}\}. \tag{15}$$

$$\boxed{\mathrm{Entity_y}} \xrightarrow{\mathit{describe}} \boxed{\mathrm{Entity_x}}$$

Entity Transitivity

Proposition 2 (Entity Transitivity). Let the following TBox T be given:

$$T := \{\mathrm{Entity_y} \sqsubseteq \exists \mathit{describe}.\mathrm{Entity_x}, \tag{14a}$$

$$\mathrm{Entity_x} \sqsubseteq \exists \mathit{present\text{--}at}.\mathrm{Situation_x}\} \tag{14b}$$

Then the following holds:

$$T' := T \cup \{\mathrm{Entity_y} \sqsubseteq \exists \mathit{present\text{--}at}.\mathrm{Situation_x}\}. \tag{15}$$

$$\begin{tikzcd}
\boxed{\mathrm{Entity_y}} \arrow[r, "\mathit{describe}"] & \boxed{\mathrm{Entity_x}} \arrow[r, "\mathit{present\text{--}at}"] & \boxed{\mathrm{Situation_x}}
\end{tikzcd}$$

Entity Transitivity

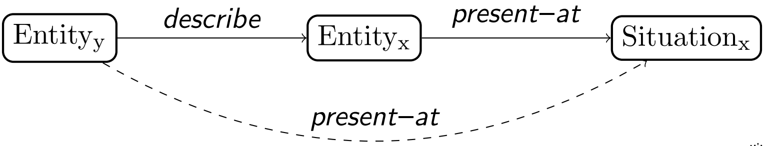
Proposition 2 (Entity Transitivity). Let the following TBox T be given:

$$T := \{\mathrm{Entity_y} \sqsubseteq \exists \mathit{describe}.\mathrm{Entity_x}, \tag{14a}$$

$$\mathrm{Entity_x} \sqsubseteq \exists \mathit{present\text{--}at}.\mathrm{Situation_x}\} \tag{14b}$$

Then the following holds:

$$T' := T \cup \{\mathrm{Entity_y} \sqsubseteq \exists \mathit{present\text{--}at}.\mathrm{Situation_x}\}. \tag{15}$$



LONDON METROPOLITAN UNIVERSITY

Entity Inheritance

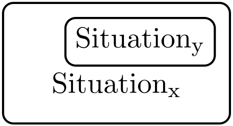
Proposition 3 (Entity Inheritance). Let the following TBox T be given:

$$T := \{\mathrm{Situation_y} \sqsubseteq \mathrm{Situation_x}, \tag{16a}$$

$$\mathrm{Entity_x} \sqsubseteq \exists \mathit{present{-}at}.\mathrm{Situation_x}\} \tag{16b}$$

Then the following holds:

$$T' := T \cup \{\mathrm{Entity_x} \sqsubseteq \exists \mathit{present{-}at}.\mathrm{Situation_y}\}. \tag{17}$$



Entity Inheritance

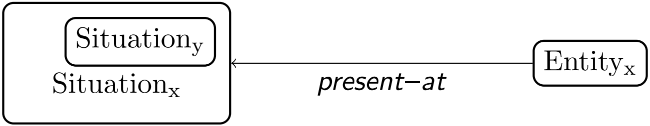
Proposition 3 (Entity Inheritance). Let the following TBox T be given:

$$T := \{\mathrm{Situation_y} \sqsubseteq \mathrm{Situation_x}, \tag{16a}$$

$$\mathrm{Entity_x} \sqsubseteq \exists \textit{present–at}.\mathrm{Situation_x}\} \tag{16b}$$

Then the following holds:

$$T' := T \cup \{\mathrm{Entity_x} \sqsubseteq \exists \textit{present–at}.\mathrm{Situation_y}\}. \tag{17}$$



Entity Inheritance

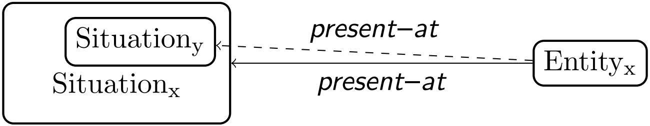
Proposition 3 (Entity Inheritance). Let the following TBox T be given:

$$T := \{\mathrm{Situation_y} \sqsubseteq \mathrm{Situation_x}, \tag{16a}$$

$$\mathrm{Entity_x} \sqsubseteq \exists \mathit{present{-}at}.\mathrm{Situation_x}\} \tag{16b}$$

Then the following holds:

$$T' := T \cup \{\mathrm{Entity_x} \sqsubseteq \exists \mathit{present{-}at}.\mathrm{Situation_y}\}. \tag{17}$$



Logical Foundations: Semantic Web Rule Language (SWRL)

SWRL Knowledge Base (K) is defined as follows: $K = (\Sigma, R)$ where Σ is KB of $\mathcal{ALC}$ and R is set of rules. The rules consist of *body* and *head* as follows:

$$body \rightarrow head$$

where the atoms are defined using conjunctions of classes $C(i)$ (concepts in $\mathcal{ALC}$) and object properties $R(i, j)$ (roles in $\mathcal{ALC}$). [2].

Example

$C(i) \rightarrow P(j)$
$Q(i) \wedge W(h, g) \wedge Z(g) \rightarrow X(j, h)$

Policy Rules

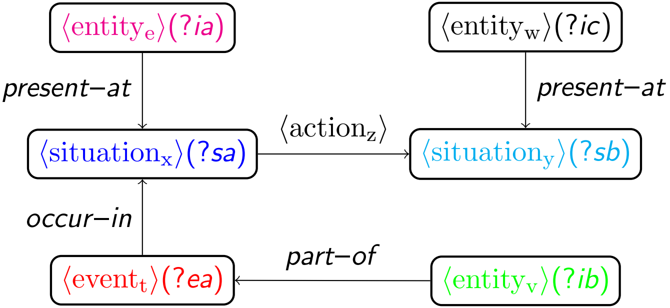
1. $\langle \mathrm{situation}_{\mathrm{x}} \rangle(?sa) \wedge \langle \mathrm{entity}_{\mathrm{e}} \rangle(?ia) \wedge \mathit{present\text{–}at}(?ia, ?sa) \wedge \ldots \wedge \langle \mathrm{situation}_{\mathrm{y}} \rangle(?sb) \wedge \langle \mathrm{action}_{\mathrm{z}} \rangle(?sa, ?sb) \rightarrow \langle \mathrm{entity}_{\mathrm{w}} \rangle(?ib) \wedge \mathit{present\text{–}at}(?ib, ?sb) \wedge \ldots$

$$
\begin{tikzcd}
\boxed{\langle \mathrm{entity}_{\mathrm{e}} \rangle(?ia)} \arrow[d, swap, "\mathit{present\text{–}at}"] & & \boxed{\langle \mathrm{entity}_{\mathrm{w}} \rangle(?ib)} \arrow[d, "\mathit{present\text{–}at}"] \\
\boxed{\langle \mathrm{situation}_{\mathrm{x}} \rangle(?sa)} \arrow[rr, "\langle \mathrm{action}_{\mathrm{z}} \rangle"] & & \boxed{\langle \mathrm{situation}_{\mathrm{y}} \rangle(?sb)}
\end{tikzcd}
$$

LONDON METROPOLITAN UNIVERSITY

Policy Rules

2. $\langle \text{situation}_{\text{x}} \rangle (?sa) \wedge \langle \text{entity}_{\text{e}} \rangle (?ia) \wedge present\text{–}at(?ia, ?sa) \wedge$
$\langle \text{event}_{\text{t}} \rangle (?ea) \wedge occur - in(?ea, ?sa) \wedge \ldots \wedge$
$\langle \text{entity}_{\text{v}} \rangle (?ib) \wedge part\text{–}of(?ib, ?ea) \wedge \ldots \wedge$
$\langle \text{situation}_{\text{y}} \rangle (?sb) \wedge \langle \text{action}_{\text{z}} \rangle (?sa, ?sb) \rightarrow$
$\langle \text{entity}_{\text{w}} \rangle (?ic) \wedge present\text{–}at(?ic, ?sb) \ldots$



Case scenario

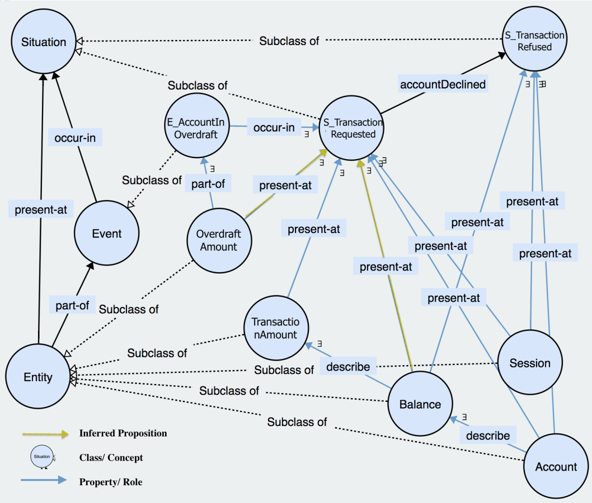


Figure: Transaction declined due to insufficient funds

Case scenario: TBox

$$
\begin{array}{c}
S\_TransactionRequested \sqsubseteq Situation,\ S\_TransactionRefused \sqsubseteq Situation,\\
Account \sqsubseteq Entity,\ Session \sqsubseteq Entity,\ Balance \sqsubseteq Entity,\\
TransactionAmount \sqsubseteq Entity,\ OverdraftAmount \sqsubseteq Entity,\\
Account \sqsubseteq \exists describe.Balance,\ Balance \sqsubseteq \exists describe.TransactionAmount,\\
Account \sqsubseteq \exists present\text{–}at.S\_TransactionRequested,\\
Session \sqsubseteq \exists present\text{–}at.S\_TransactionRequested,\\
TransactionAmount \sqsubseteq \exists present\text{–}at.S\_TransactionRequested,\\
E\_AccountInOverdraft \sqsubseteq Event,\\
OverdraftAmount \sqsubseteq \exists part\text{–}of.E\_AccountInOverdraft,\\
E\_AccountInOverdraft \sqsubseteq \exists occur\text{–}in.S\_TransactionRequested,\\
Account \sqsubseteq \exists present\text{–}at.S\_TransactionRefused,\\
Session \sqsubseteq \exists present\text{–}at.S\_TransactionRefused,\\
Balance \sqsubseteq \exists present\text{–}at.S\_TransactionRefused.
\end{array}
$$

Table: TBox T

Case scenario: RBox

$$
\begin{array}{|c|}
\hline
\exists accountDeclined.\top \sqsubseteq S\_TransactionRefused, \\
\top \sqsubseteq \forall accountDeclined.S\_TransactionRequested, \\
\exists occur{-}in.\top \sqsubseteq Event, \\
\top \sqsubseteq \forall occur{-}in.Situation, \\
\exists part{-}of.\top \sqsubseteq Entity, \\
\top \sqsubseteq \forall part{-}of.Event, \\
\exists present{-}at.\top \sqsubseteq Entity, \\
\top \sqsubseteq \forall present{-}at.Situation. \\
\hline
\end{array}
$$

Table: RBox R

Case scenario: The Rule

$S\_TransactionRequested(?sa) \wedge Balance(?ib) \wedge present\text{–}at(?ib, ?sa) \wedge Session(?is) \wedge present\text{–}at(?is, ?sa) \wedge Account(?ia) \wedge present\text{–}at(?ia, ?sa) \wedge TransactionAmount(?it) \wedge present\text{–}at(?it, ?sa) \wedge E\_AccountInOverdraft(?ea) \wedge occur - in(?ea, ?sa) \wedge OverdraftAmount(?io) \wedge part\text{–}of(?io, ?ea) \wedge S\_TransactionRefused(?sb) \wedge$ **AccountDeclined(?sa,?sb)** $\rightarrow$
$Balance(?ib) \wedge present\text{–}at(?ib, ?sb) \wedge Session(?is) \wedge present\text{–}at(?is, ?sb) \wedge Account(?ia) \wedge present\text{–}at(?ia, ?sb)$

S_Situation (?sa), Entity (?ib), E_Event (?ea)

Next: Analytical Level

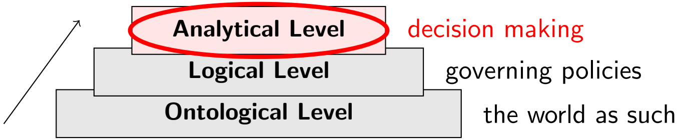


Figure: Multi- level Model for Analysis

Analytical Level: Accessibility, Vulnerability and Risks

- Use graph theory: concepts as nodes and roles as edges (Markov decision process).
- Define vulnerable state/ situation throughout the journey, sequesce of actions.
- Apply probablity/ Bayesian theory to assess risks.

Graphical Representation

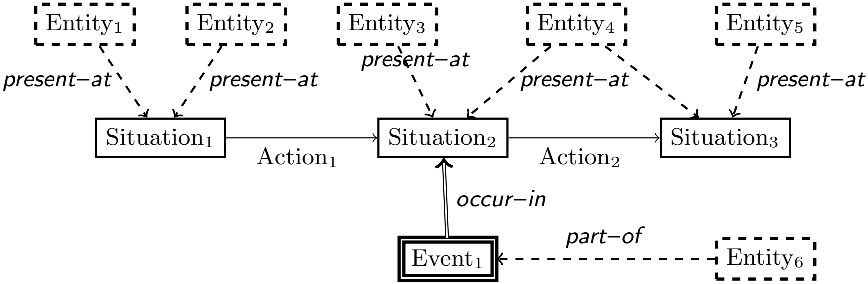


Figure: A graphical representation of two-step journey

Conclusion and Further Work

- We outlined a *multi-level framework for modelling*, simulation and analysis of such systems using formal methods based on combining description logic, clausal logic and graph theory.
- We presented *ontological and logical considerations for knowledge representation* and processing of transactions in dynamic systems.
- Our framework provides *theoretical basis* for solving some of the hard problems in modelling dynamic behaviour when utilize the concept of state, by proper distinction between the static characteristics of the situations and the possible side effect of the actions on them.
- Currently, we are working on an extension of the framework with risk analysis capabilities, based on Bayesian theory.

LONDON METROPOLITAN UNIVERSITY

References

Bataityte, K., Vassilev, V., Gill, O.J.: Ontological foundations for vulnerability analysis of security policies (2020), [to appear]

Lawan, A., Rakib, A.: The semantic web rule language expressiveness extensions-a survey (03 2019)

Roşu, G.: Cyber security breaches survey 2018: Main report. Department for Digital, Culture, Media and Sport (Apr 2018), https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2018, [Online; accessed 21-February-2019]

Sãnchez, D., Cavero, J.M., Marcos Martnez, E.: The Road Toward Ontologies, vol. 14, pp. 3–20. Springer US (2007)

Szeredi, P., Lukácsy, G., Benkő, T.: The Semantic Web Explained: The Technology and Mathematics Behind Web 3.0. Cambridge University Press, New York, NY, USA (2014)

Tsarkov, D., Horrocks, I.: Efficient reasoning with range and domain constraints. In: Proceedings of the 2004 International Workshop on Description Logics (DL2004) (2004)

LONDON METROPOLITAN UNIVERSITY