ESORICS OSLO 2017
11.-15. September

1st International Workshop on SECurity and Privacy Requirements Engineering,
14 – 15 September 2017, Oslo, Norway

Evaluation of a Security and Privacy Requirements Methodology using the Physics of Notation

V. Diamantopoulou, M. Pavlidis, H. Mouratidis
School of Computing, Engineering and Mathematics
University of Brighton
United Kingdom

University of Brighton

Presentation Outline

- Introduction
- Secure Tropos methodology
- Visual Notation Principles – Theory of Notation
- Methodology evaluation
- Conclusions – Future steps

Introduction

- Security and privacy requirements engineering methodologies
  - provide techniques, methods and norms for dealing with each task, during the early stages of the Information Systems (IS) development cycle
  - supply researchers with existing information about security and privacy requirements, providing the necessary context to operate
  - should be specified at the early stages of an IS development process
    - more efficient building of such requirements
    - more robust designs

Introduction

- Visual notations
  - Are considered as a main element of each methodology
  - Are used in all stages of the Software Engineering process
    - From requirements engineering to maintenance
  - Play critical role in communicating with end users and customers
    - Convey information more effectively
    - Facilitate human communication
- Diagrams
  - Convey information more concisely and precisely
  - Information presented visually: likely to be remembered

Visual syntax

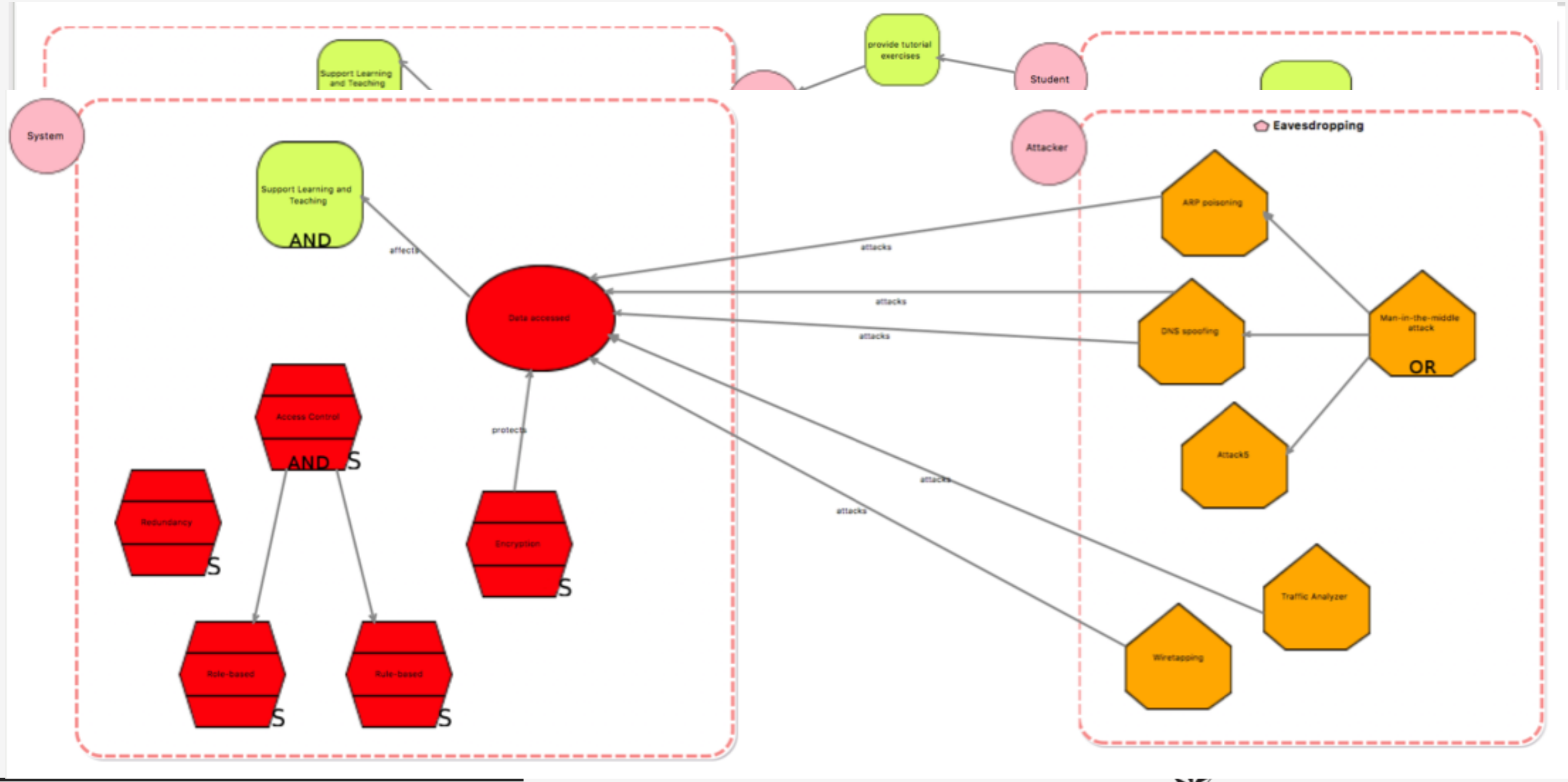
- Major contribution on the understanding of each methodology
  - Especially by novices
- Researchers underestimate its importance
  - More effort is spent on designing semantics (i.e. what concepts to include, what they mean)
  - Visual syntax (i.e. how to visually represent these concepts) is considered at a later stage

Our contribution

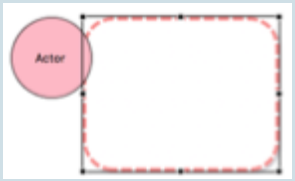
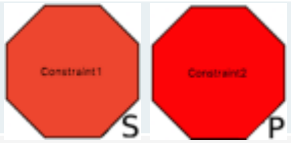
- Evaluation of an already existing security and privacy requirements engineering methodology
- Examination of its graphical notation
  - For further improvement

Secure Tropos methodology

- A structured approach for goal-oriented security and privacy requirements modelling
- Adopts i* framework concepts
  - Standard goal-oriented requirements engineering concepts (e.g., *actors, goals, dependencies*)
- Security related concepts (e.g., *security constraints, threats, security mechanisms*)
- Supports the analysis and design activities in the software development process
  - Capturing of:
    - Early requirements
      - Modelling of the environment of the system
    - Late requirements
      - Modelling of the system itself


provide tutorial exercises
Student
Support Learning and Teaching
System
Support Learning and Teaching
AND
affects
Data accessed
Access Control
AND
S
Redundancy
S
protects
Encryption
S
Role-based
S
Rule-based
S
Attacker
Eavesdropping
ARP poisoning
attacks
attacks
attacks
DNS spoofing
Man-in-the-middle attack
OR
AttackS
attacks
attacks
Traffic Analyzer
Wiretapping

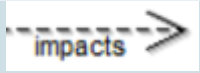
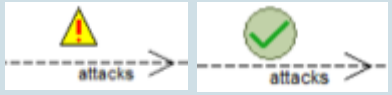
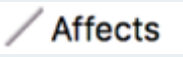
Secure Tropos Concepts

Concept	Notation
Actor	
(Hard) Goal	
Soft Goal	
Plan	
Resource	
Constraint	

Concept	Notation
Mechanism	
Threat	
Attacker	
Vulnerability	
Attacks Method	

Secure Tropos Relationship Types

Relation class	Notation
Dependency	
And	
Or	
Contribution	
Restricts	
Satisfies	

Relation class	Notation
Impacts	
Mitigates	
Attacks	
Affects	
Protects	

Visual Notation Principles – Theory of Notation

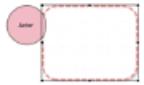
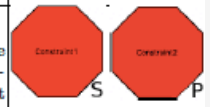
1. **Principle of Semiotic Clarity**
   - One-to-one correspondence between semantic constructs and graphical symbols
   - Precision, expressiveness and parsimony
2. **Principle of Perceptual Discriminability**
   - Different symbols should be clearly distinguishable
   - Accurate graphical symbols
3. **Principle of Semantic Transparency**
   - Visual representations whose appearance suggests their meaning
4. **Principle of Complexity Management**
   - Diagrams' notation should deal with complexity
   - *Modularisation* (certain semantic constructs) and *hierarchy* (different levels of abstraction)

Visual Notation Principles – Theory of Notation

5. **Principle of Cognitive Integration**
   - Integration of information from different diagrams
   - *Conceptual* (assembly information) and *perceptual* (easy navigation) *integration*
6. **Principle of Visual Expressiveness**
   - Full range and capacities of visual variables
   - Related to Perceptual Discriminability → they both contribute to understandability
7. **Principle of Dual Coding**
   - Use of text in the modelling process
   - Capturing of human abilities across their full spectrum of spatial and verbal abilities
8. **Principle of Graphic Economy**
   - Careful number of different graphical symbols
9. **Principle of Cognitive Fit**
   - Use of different visual dialects (different audiences or different representational medium)

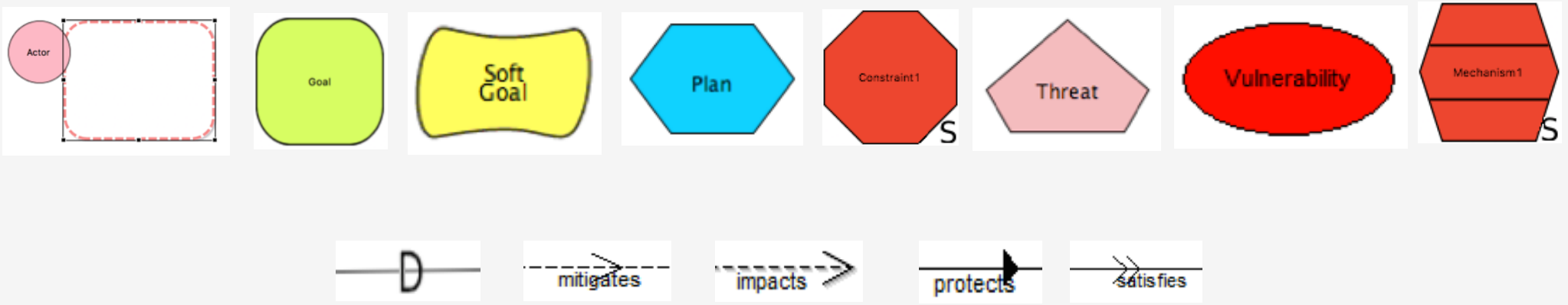
Secure Tropos Evaluation

#	Principle	Evaluation	Satisfaction
1	Semiotic Clarity	• One-to-one correspondence between symbols and content. • Contribution to precision and efficient expressiveness of the symbols, avoiding ambiguity and misinterpretation	

Concept	Description	Notation
Actor	Active entities that carry out actions to achieve goals by exercising its know-how. The term actor refers generically to any unit to which intentional dependencies can be ascribed. An actor interacts with other actors not only through actions or information flows but also relate to each other at an intentional level. Actors depend on each other to achieve goals, perform tasks, and furnish resources. While each actor has strategic goals to pursue, they are achieved through a network of intentional dependencies	
(Hard) Goal	A condition or state of affairs to be achieved. An actor can choose freely 'among different ways to achieve a goal. Represents and intentional desire of an actor, the specifics of *how* the goal is to be satisfied is not described by the goal. This can be described through task decomposition.	
Soft Goal	A goal that does not have clear criteria on whether it has been achieved.	
Plan	The way to achieve a goal.	
Resource	An informational or physical entity.	
Constraint	A restriction on an actor's function. There are two types of Constraints, namely Security and Privacy. Additionally, a Constraint is related to an Objective e.g., Confidentiality, Integrity, Authentication, etc.	

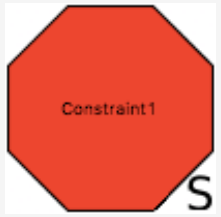
Secure Tropos Evaluation

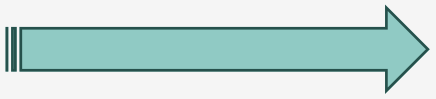
#	Principle	Evaluation	Satisfaction
2	Perceptual Discriminability	• Use of different shapes and colours (substantial visual distance) • Use of elements that discriminate the concepts (arrows, dashed lines) • The same colour for more than one concepts is being used • Use of text (labels) that differentiate most of the relationship types	

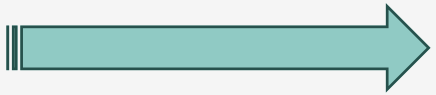


Secure Tropos Evaluation

#	Principle	Evaluation	Satisfaction
3	Semantic Transparency	• "Constraint": Stop sign; familiar to anyone, can be interpreted as the criticality of a situation • "Attack link": i) red exclamation mark, ii) green tick	







The identified vulnerability has **not** been mitigated by a security/ privacy mechanism

All possible attacks **have been** mitigated

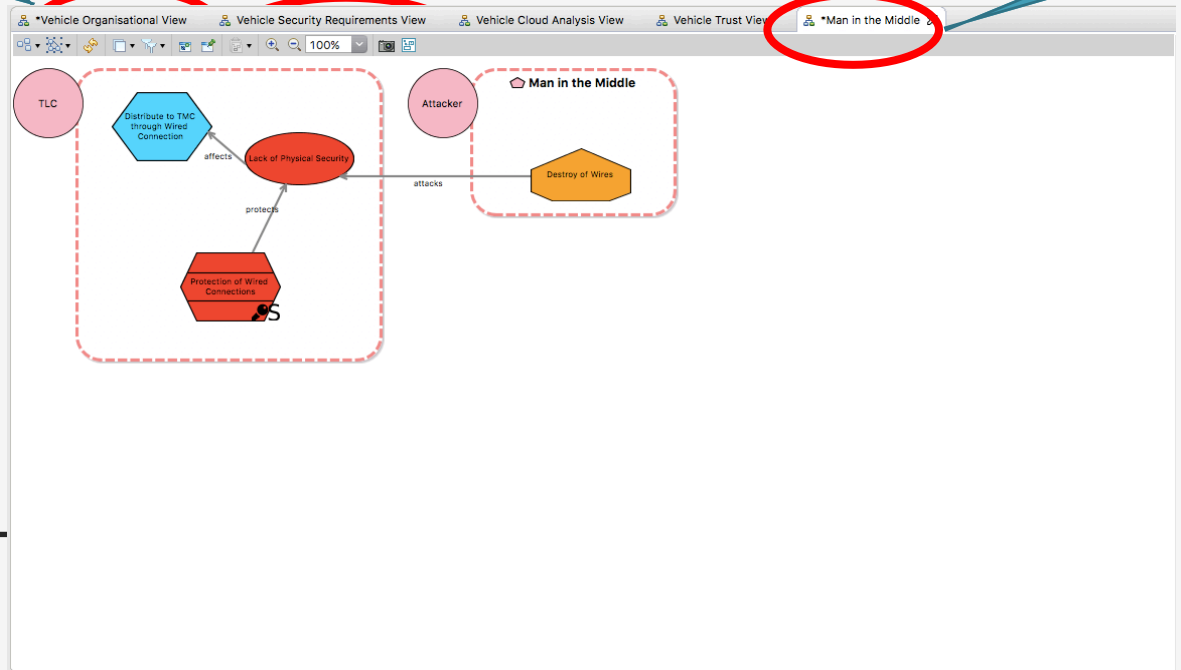
Secure Tropos Evaluation

#	Principle	Evaluation	Satisfaction
4	Complexity Management	• The diagrams follow *hierarchy structure* for the representation of goals → readability • *Modularisation:* Different views where the information is grouped according to these perspectives (organisational, requirements, attacks) [illegible]resented in an additional view → reada [illegible]this principle is not satisfied (problem[illegible] [illegible]ms	

Organisational View

Requirements View

Attacks View



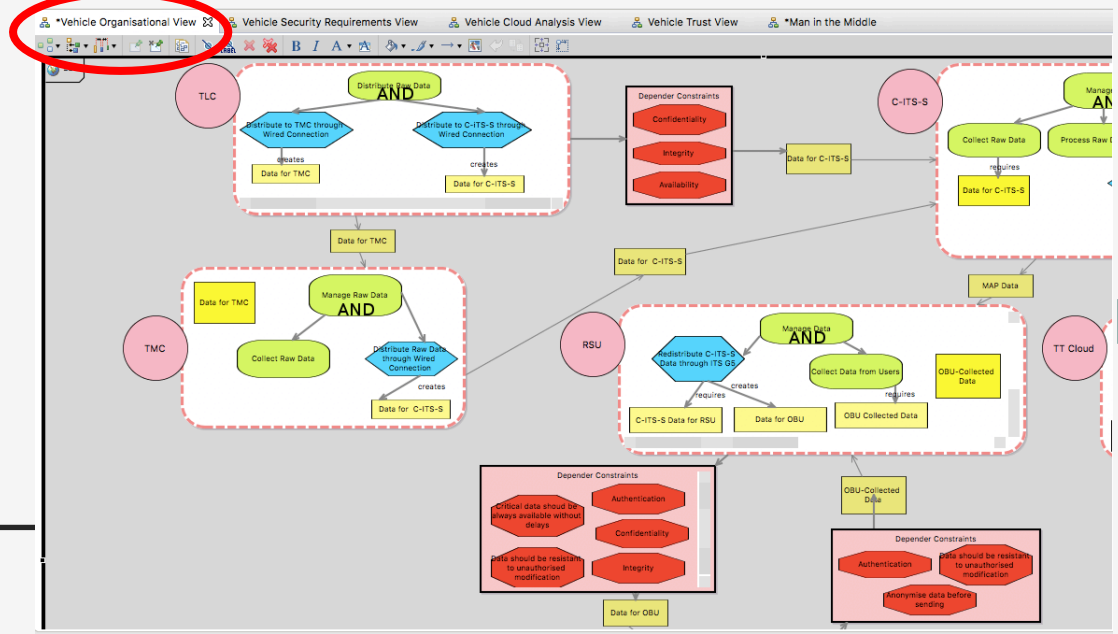
University of Brighton

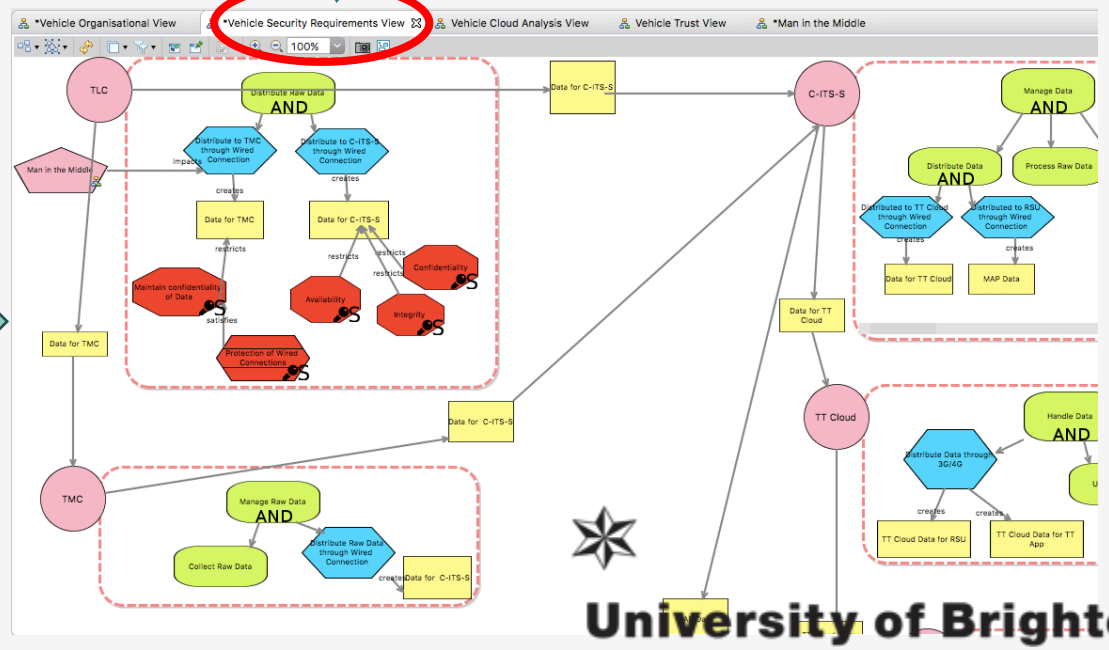
Secure Tropos Evaluation

#	Principle	Evaluation	Satisfaction
5	Cognitive Integration	• Representation of the system through multiple diagrams; each one responsible for specific analysis. Users have to parse all the information for a holistic knowledge of the system. *Contribution to the demanded effort* for keeping track of where they are. • The concepts that are introduced in the Org and are essential for the other views, are *automatically* i tribution to the realisation of the core concepts of the analysed system	✓

Organisational View

Requirements View

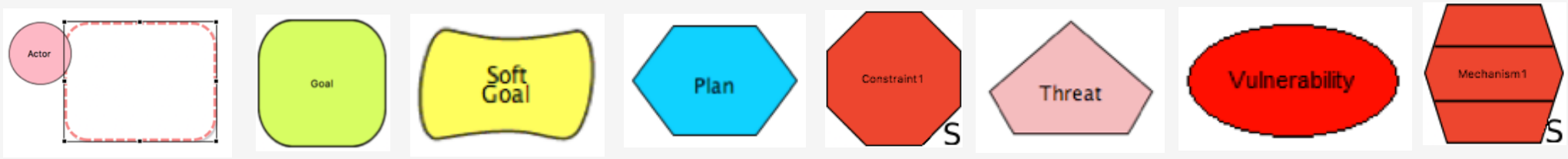




University of Brighton

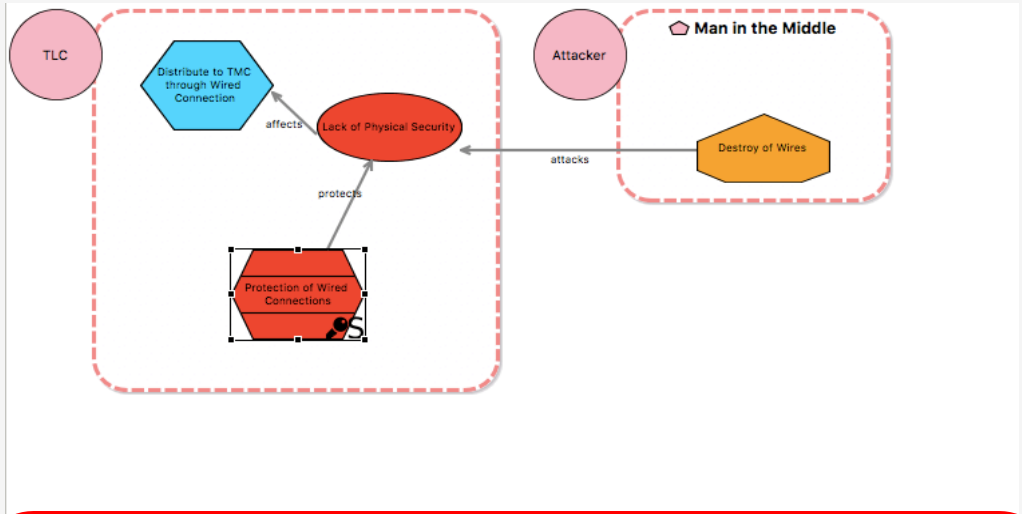
Secure Tropos Evaluation

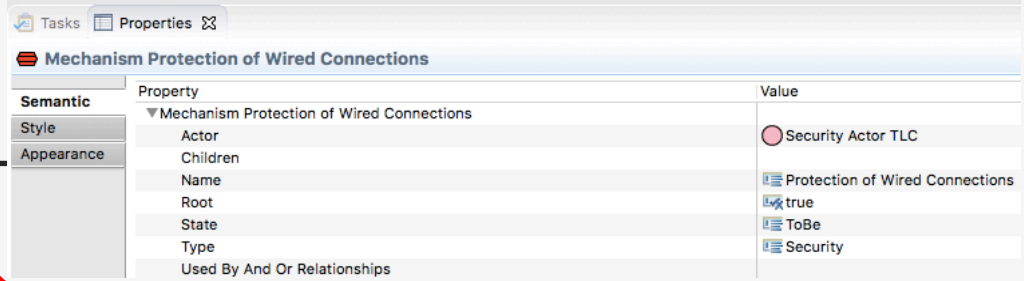
#	Principle	Evaluation	Satisfaction
6	Visual Expressiveness	• Use of colours for the distinguish of each concept → Contribution to the comprehension of the models, avoiding technical or human misunderstandings • Use of shapes (rectangle, round rectangle, cycle, 6-7-8-gone, diamond shape, ellipse) • The variety of shapes is the less effective, regarding human visual processing. Curved and 3d objects have to be preferred • Ratio of graphical encoding/textual encoding: textual is used in all of the relationship notations	



Secure Tropos Evaluation

#	Principle	Evaluation	Satisfaction
7	Dual Coding	• Each concept is supported by the 'Properties Panel', which provides information.	✓

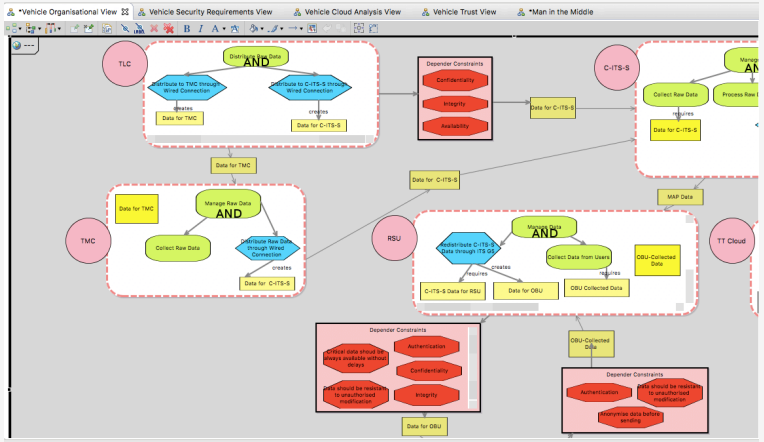


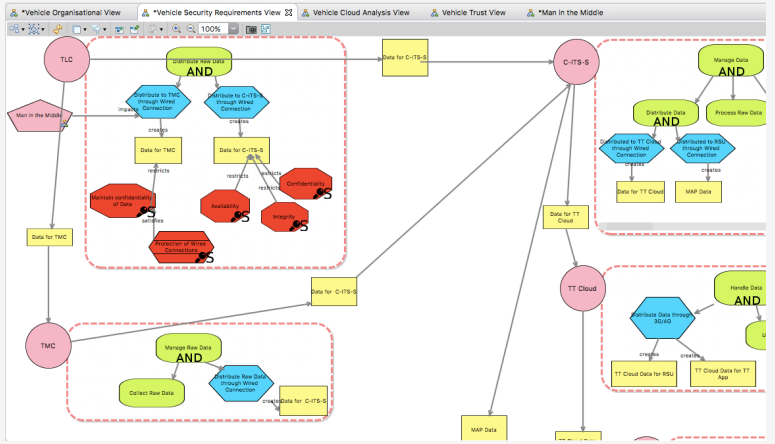


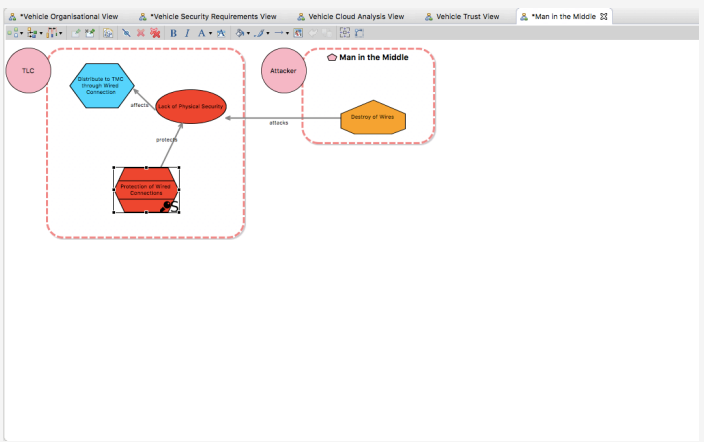
University of Brighton

Secure Tropos Evaluation

#	Principle	Evaluation	Satisfaction
8	Graphic Economy	• The use of different views allows users to focus on specific perspective of the examined system • The diagrams are effectively presented, they distinguish information according to the focus of each analysis part	✓







Secure Tropos Evaluation

#	Principle	Evaluation	Satisfaction
9	Cognitive Fit	• No provision of two versions • Does not cover the level of expertise of users	

Conclusions

- The language can be improved, focusing in the revision of specific elements
  - contribution to the overall communication of the language with its users
- This evaluation can also be applied to other security and privacy requirements engineering methodologies
  - Their evaluation and comparison can reveal useful findings
  - These findings can be used for the development of **guidelines** for the improvement of their visual syntax

Future steps

- Empirical evaluation
  - Involvement of external practitioners
  - Distinguish of users to experts and novices
    - Record their perception regarding the *design goals* (simplicity, aesthetics, expressiveness, naturalness) and *cognitive effectiveness* (speed, ease, accuracy)

Thank you for your attention

Contact me at: v.diamantopoulou@brighton.ac.uk

Visit us at: www.sense-brighton.eu

University of Brighton